# 2025 NATIONAL RISK ASSESSMENT OF MONEY LAUNDERING

Observation period: 2020 – 2023

THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of Justice

# Contents

# 1. Introduction

Luxembourg's first National Risk Assessment (NRA) of money laundering and terrorist financing was adopted in September 2018 (2018 NRA) and provided an assessment of Luxembourg's situation concerning its money laundering and terrorist financing (ML/TF) risks as of year-end 2017. In the course of 2020, the NRA was updated (2020 NRA) to reflect Luxembourg's situation as of year-end 2019. It was adopted by the National Prevention Committee on money laundering and terrorist financing (NPC) on 15 September 2020.

To further enhance its understanding of higher risk sectors, the NPC conducted specific risk assessments, so-called vertical risk assessments (VRAs). In this respect, VRAs on virtual asset service providers (VASPs), legal persons and legal arrangements and on TF were carried out. These risk assessments are publicly available, in both English and French, on the website of the Ministry of Justice (MoJ)[1] and of other relevant authorities and stakeholders.

The fight against ML and TF shares a common legal framework. However, ML and TF have their own specificalities that are better taken into consideration when analysed in specific risk assessments. For instance, even if ML and TF can exploit the same vulnerabilities of a product or service, ML and TF differ in their nature, source and purpose. Additionally, as illustrated by the 2018 and 2020 NRA on ML/TF and the 2022 TF VRA, the level of ML threat level in Luxembourg differs from the TF threat level. A separate analysis allows for a better understanding of the particular drivers of each type of risks. This approach facilitates the implementation of more targeted and ultimately more effective mitigation actions.

Taking this into account, the NPC decided to update the 2020 ML/TF NRA by carrying out two separate NRAs, one specifically on ML and the other on TF:

- The NRA on ML was carried out using quantitative and qualitative data related to years 2020 to 2023. In April 2025 the NPC approved the publication of this ML specific update, hereafter referred to as the 2025 NRA of ML;
- The NRA on TF will be carried out subsequently, leveraging on the 2022 TF VRA methodology and using quantitative and qualitative data related to years 2021-2024.

The ultimate goal of these risk assessments is to update the understanding of ML/TF risks and to allow a risk-based approach (RBA) at all levels.

[1] MoJ website, link.

# 2. Executive summary

This report constitutes Luxembourg's latest update of its national risk assessment of ML[2]. This 2025 NRA was carried out under the direction of the MoJ and the NPC approved its publication on 28 April 2025. It formalises Luxembourg's common understanding of ML risks and forms the basis of the RBA at all levels, from policy makers and law enforcement authorities (LEAs) to supervisors, obliged entities and professionals, to ensure that ML prevention, detection and mitigation measures are commensurate with the risks identified.

As explained in the introduction above, this NRA update focuses on ML risks. In terms of methodology, it follows the same approach as the previous NRAs conducted in 2020 and 2018. It consists of first assessing the inherent risk resulting from the main ML threats to which Luxembourg is exposed and the vulnerabilities of the various (sub-)sectors covered by the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended (2004 AML/CFT Law). Mitigation measures to reduce inherent risks are then taken into account to determine the residual risks.

The main findings of this 2025 NRA are as follows:

- In terms of threats:
    - ML of proceeds of foreign crimes is the most significant ML threat for Luxembourg, given its position as a global financial centre. Fraud and forgery, tax crimes, corruption and bribery continue to be the main external threats;
    - Exposure to domestic ML, derived from the proceeds of primary offences committed in Luxembourg, is much lower given the country's low level of criminality. Fraud and forgery, robbery and theft as well as drug trafficking are the main domestic threats;
    - Although terrorism and TF are predicate offences to ML, the related threat will be considered in a separate specific NRA of TF, as explained in the introduction.
- In terms of vulnerabilities:
    - Within the financial sector, banks[3], investment firms[4], e-money institutions (EMIs), payment institutions (PIs), Specialised Professionals of the Financial Sector (PFSs) providing corporate services, VASPs[5], and life insurance undertakings were assessed as having a "High" inherent risk level;
    - Within the non-financial sector, the inherent risk levels for all legal and accounting professions remain "High", with the exception of the audit profession and bailiffs, which were assessed to bear a "Medium" inherent risk;

[2] The first NRA, adopted in September 2018, link, was updated in 2020, link.

[3] Excepted Custodians and sub-custodians (incl. Central Securities Depositories) that have a "Medium" inherent risk level.

[4] Excepted 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 that have a "Medium" inherent risk level.

[5] VASPs were assessed in 2020 in a dedicated vertical risk assessment, link.

- With respect to legal persons and legal arrangements, the 2025 NRA leverages the approach and findings of the dedicated VRA (2022 LPs/LAs VRA)[6]. Legal arrangements were assessed as bearing the highest inherent risk, followed by *Sociétés commerciales*.

As noted above, the mitigating factors put in place within and across sectors reduce the level of inherent risk to a level of residual risk.

As a financial centre, Luxembourg contributes to international efforts and demonstrates its full commitment to the fight against ML and TF. Following the on-site visit for mutual evaluation of Luxembourg by the Financial Action Task Force (FATF) in November 2022, the FATF published on 27 September 2023 its Mutual Evaluation Report of Luxembourg[7], recognising that Luxembourg has "a solid anti-money laundering and counter-terrorist financing framework and a good understanding of its money laundering and terrorist financing risks"[8].

[6] MoJ, *Legal persons and legal arrangements ML/TF vertical risk assessment*, 2022, link.

[7] FATF, *Anti-money laundering and counter-terrorist financing measures, Luxembourg, Mutual Evaluation Report, 2023,* link.

[8] FATF, Luxembourg's measures to combat money laundering and terrorist financing, link.

# 3. Luxembourg context

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 km$^2$, it is one of the smallest sovereign states in Europe.

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.

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.

**Demographic structure**

On the 1 January 2024, Luxembourg counts 672 050 inhabitants. Although among the least populous countries in the EU, the number of habitants has increased by around 31% compared to 2011.

In the beginning of 2024, people from EU Member States (other than Luxembourg) account for 37% of the resident population and 77% of the foreign population living in the Grand-Duchy. The Portuguese nationality is the first foreign nationality in the country with 90 915 persons (13,5% of the total population) followed by the French (7,3%), Italian (3,7%) and Belgian (2,8%) nationalities[9]. 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)[10].

Similar to the situation described in the 2020 NRA, the unemployment rate remains low (around 5%) and 44% of Luxembourg's workforce are non-residents living in France, Germany or Belgium and commuting to Luxembourg for work (227 799 out of 516 304 in November 2022)[11]. Luxembourgish, French and German are the three official languages. English is used in certain professional environments, notably in banking and finance.

**Luxembourg's economy**

Luxembourg's economy is open, dynamic and fast growing with a gross domestic product (GDP) at market prices of EUR 79,309 billion in 2023, thus contributing to 0,46% of the total EU GDP in 2023[12].

[9] LUStat, Population by nationalities in detail on 1st January, link retrieved on 25 September 2024.
[10] STATEC, link. Note that data refers to the most recent population census in 2021.
[11] EURES, Labour market information, link.
[12] Eurostat, Gross domestic product at market prices, link retrieved on 17 February 2025.

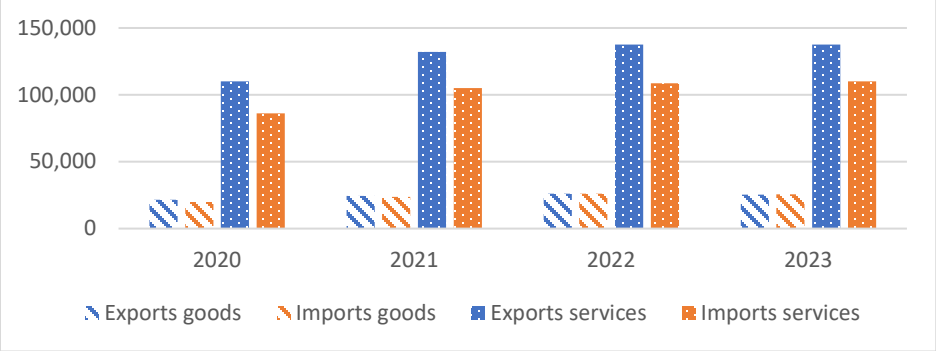
**Table 1: EU27 vs. Luxembourg real GDP growth rate (change vs. base year), 2018 – 2023**[13]

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2018 - 2023 |
|---|---|---|---|---|---|---|---|
| EU27 | 2,1 | 1,8 | -5,6 | 6,0 | 3,4 | 0,5 | 1,37 |
| Luxembourg | 1,2 | 2,9 | -0,9 | 7,2 | 1,4 | -1,1 | 1,78 |

In 2023, Luxembourg continued to have the highest real GDP per capita among the EU Member States, with approximately EUR 83 320, almost 3 times above the EU average (EUR 28 930)[14]. This is partly 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.

Luxembourg's current account is heavily influenced by the importation and exportation of services (especially services related to financial and insurance activities). Whereas the import and export of goods maintains an overall balance, it can be deducted from the figure below that Luxembourg is essentially an export country of services.

**Figure 1: Annual current account of Luxembourg (in millions of euros; BPM6 methodology)**[15]




Taking a closer look at Luxembourg's key activities, financial and insurance sectors account for the biggest share of Luxembourg's economy with around 24% of the national GDP being generated by the said sector. Other important sectors of Luxembourg's economy are outlined in Table 2. A brief description of key sectors, such as the Luxembourg financial and insurance sector, the information and communication sector as well as the transportation and storage sector, is provided below.

Note that a description of real estate activities is included in section 6.3.1. Professional, scientific and technical activities encompass legal activities and accounting, bookkeeping and auditing activities, which are described in sections 6.3.5 and 6.4.

[13] Eurostat, Real GDP Growth Rate – volume, link retrieved on 12 July 2024.
[14] Eurostat, Real GDP per Capita, link retrieved on 12 July 2024.
[15] LUStat, Annual current account of Luxembourg (in millions of euros ; BPM6 methodology), link retrieved on 12 July 2024.

**Table 2: Luxembourg economy breakdown (Gross value added per industry), 2020 – 2023**[16]

| Activities | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|
| Financial and insurance activities | 25,1% | 25,4% | 24,3% | 23,5% |
| Professional, scientific and technical activities | 10,5% | 11,1% | 12,0% | 12,5% |
| Wholesale and retail trade, repair of motor vehicles and motorcycles | 8,7% | 8,6% | 8,7% | 8,6% |
| Real estate activities | 8,0% | 7,6% | 7,4% | 7,7% |
| Human health and social work activities | 6,6% | 6,7% | 6,7% | 7,2% |
| Public administration and defence, compulsory social security | 6,5% | 6,2% | 6,3% | 7,0% |
| Construction | 5,6% | 5,4% | 5,7% | 5,7% |
| Information and communication | 5,5% | 5,2% | 5,0% | 5,1% |
| Education | 4,5% | 4,2% | 4,2% | 4,5% |
| Transportation and storage | 5,6% | 6,2% | 6,5% | 4,5% |
| Administrative and support service activities | 3,7% | 3,9% | 4,1% | 4,3% |
| Manufacturing | 5,4% | 5,2% | 4,2% | 3,9% |
| Other sectors | 4,3% | 4,2% | 4,8% | 5,5% |
| **Total activities (in EUR millions)** | **58 889 (100%)** | **65 870 (100%)** | **70 568 (100%)** | **72 410 (100%)** |

*Luxembourg's financial and insurance sector*

Luxembourg is an important financial centre in the EU, ranked 19th in the Global Financial Centres Index[17] and 5th worldwide as a green financial centre[18]. The financial centre is diversified with a core focus on banking (mainly corporate banking, depositary and custody services for funds as well as private banking), investment funds (primarily asset servicing), payment services, insurance (life, non-life and reinsurance) as well as capital markets (notably listing and post-trade services). Luxembourg acts as an EU hub and competence centre for international financial institutions (FIs) in these areas[19,20].

- **Banking activity:** As of December 2023, Luxembourg counts 120 banks employing over 26 000 employees. Corporate banking, wealth management services as well as private banking 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[21].

[16] LUStat, Gross value added by activity (NaceR2)(at current prices) (in millions EUR), link retrieved on 12 July 2024.
[17] The Global Financial Centres Index 33, 2023, link.
[18] Global Green Finance Index 11, 2023, link.
[19] Luxembourg for Finance, *Luxembourg: helping finance go global,* 2023, link.
[20] Luxembourg for Finance, Homepage, link retrieved on 16 July 2024.
[21] Luxembourg for Finance, *Luxembourg: helping finance go global,* 2023, link.

- **Payment services:** Leading international players in the payments sector have chosen Luxembourg as their hub to serve the EU payments market, often in connection to the development of e-commerce platforms.
- **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 has also become a centre for all aspects of collateral managements including clearing, settlement, custody and asset servicing. The Grand-Duchy is also a centre for securitisation and structured finance vehicles.

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.

*Luxembourg's information and communication sector*

Luxembourg ranks 8th out of 27 EU Member States in the 2022 edition of the Digital Economy and Society Index (DESI). This index assesses the progress made in EU Member States in digital matters[22]. Considering the Grand-Duchy's geographical position, it is intricately connected to an international fiber network, making it an ultra-low latency hub. With a well-defined ultra-high-speed broadband strategy, its national very high-capacity network and 5G coverage are constantly increasing[23].

In 2023, Luxembourg reported the highest rates of household connection to the internet with slightly over 99% within the EU. Luxembourg internet users are also among the most active ones within the EU, with over 99% stating that they used the internet in the last 3 months (in comparison to 91% of the EU households). Consequently, the share of non-internet users is minimal with less than 0,5% (6% within the EU)[24].

Over 9 Luxembourg individuals out of 10 (91%) use a mobile device or a smart phone to connect to the internet, 65% used the laptop or tablet and 35% use a desktop computer. Furthermore, about one third indicated that they also used other mobile devices such as smart TV or smart speakers to access the internet. Most of them used these devices for texting, video calls or instant messaging (82%).

With respect to the use of eGovernment and the digital public services, Luxembourg is ranked 6th with over 70% of internet users having interacted with public authorities. Luxembourg also reported the highest rate of internet users having requested official documents or certificates (51% in comparison to an EU average of 18%).

[22] European Commission, *Luxembourg in the Digital Economy and Society Index,* link.
[23] Luxembourg – let's make it happen, Technological environment*,* link.
[24] Eurostat, Individuals – internet use, link.

The share of internet users for buying or ordering goods or services is also relatively high in Luxembourg, with over 80% internet users having bought or ordered something online. The EU average amounts to 70%[25].

Luxembourg has also the highest density of Tier IV data centres in Europe. Note that Tier IV represents the highest industry standard for reliability and efficiency for datacentres[26].

It should also be noted that Luxembourg has developed a cybersecurity hub and is among the front-runner countries for its cyber-security commitment, both in Europe and in the world. The Global Security Index (2020) assessed that the Grand-Duchy ranks 13th worldwide and 6th in Europe for its cybersecurity commitment. Based on data from December 2019, Luxinnovation and the Luxembourg House of Cybersecurity estimate that Luxembourg counts over 300 cybersecurity companies with around a quarter having cybersecurity as their core business[27].

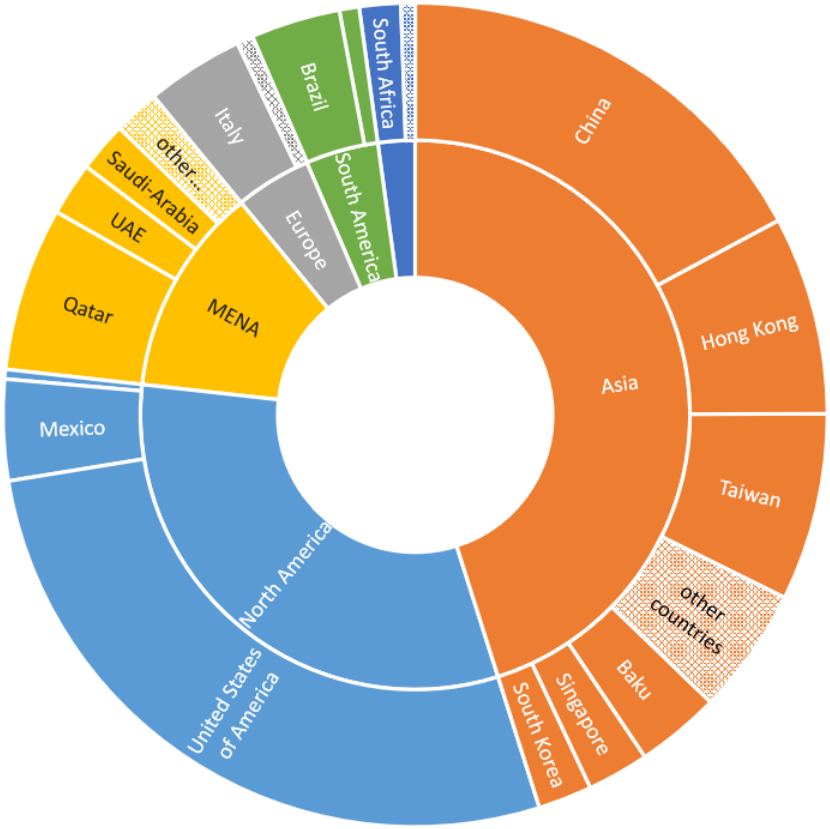
*Luxembourg's transportation and storage sector*

Luxembourg is member of the Schengen Area and around 70% of the EU GDP is located within 700 km of Grand-Duchy[28]. Luxembourg has a global air-cargo connectivity, a rail freight and a multimodal terminal in Bettembourg. Luxembourg has been ranked 26th out of 139 countries in The Logistics Performance Index[29].

- **Air freight:** Luxembourg has an air-cargo network including more than 100 destinations on six continents from the airport Cargo Centre. Luxembourg is the headquarters of Cargolux Airlines and is often a major European hub for other air-freight carriers (China Airlines, Emirates, Yangtze River Express, Silkway Airlines, Atlas Air et Qatar Airways)[30]. In 2022, Luxembourg transported 969 105 tons of air freight and mail with almost 96% accounting for international extra EU transports. In terms of transported freight (in tons), it ranks 6th among the EU[31]. In a similar vein, the distance bands of the Luxembourg Cargo airport and the destination/recipient airport is located over 2 000 kilometers away for 90% of the transported freight[32]. The figure below outlines the geographical distribution of the main partner airports (in terms of transported weight). Whereas the United States of America is the country with which Luxembourg has imported/exported most airfreight (over 1,2 million tons between 2019 and 2023), Luxembourg exchanges also a significant amount of airfreight with the Asian continent (over 2 million tons between 2019 and 2023), especially with countries such as China (about 762 000 tons), Hong Kong (about 345 tons) and Taiwan (about 327 tons).

[25] Eurostat, Digital economy and society statistics, households and individuals, link.
[26] Luxembourg – let's make it happen, Technological environment, link.
[27] Luxinnovation, Luxembourg Cybersecurity Ecosystem, link retrieved on 11 July 2024.
[28] Eurostat, Gross domestic product at market prices, link retrieved on 16 July 2024.
[29] The World Bank, The Logistics Performance Indicator 2023, link.
[30] Single window for logistics Luxembourg, link retrieved on 16 July 2024.
[31] Eurostat, Air transport statistics, link retrieved on 16 July 2024.
[32] Eurostat, Freight and mail air transport by aircraft model, distance bands and transport coverage, link retrieved on 16 July 2024.

**Figure 2: Freight and mail air transport routes between partner airports and airports in Luxembourg, 2019 - 2023[33]**




- **Rail freight:** The Bettembourg multimodal platform links Luxembourg and its neighboring countries to the rest of the Europe by road and rail with access to Italian, Spanish, Eastern European, UK and Scandinavian markets[34]. In terms of transported freight (in million tons), Luxembourg was situated in 2022 among the lower end of the scale of EU countries with a total of 3 464 million tons of transported freight via rail. It should be noted that 23% of transported freight (in terms of weight transported) were national, 73% international and 4% transit[35,36]. Almost all imports (1 495 million tons out of 1 503 million) were imported from the EU. More precisely, 996 million tons were imported from Germany (i.e. 66% of all imports), 315 million tons from Belgium (i.e. 21%) and 112 million tons from France (i.e. 7%). In 2022, the number of loaded wagons in the Grand-Duchy amounted to 31 584[37].

[33] Eurostat, Freight and mail air transport routes between partner airports and main airports in Luxembourg [avia_gor_lu__custom_12176738], link retrieved on 16 July 2024.
[34] Single window for logistics Luxembourg, link retrieved on 16 July 2024.
[35] Eurostat, Railway Freight Transport statistics, link retrieved on 16 July 2024.
[36] LuStat, Freight Traffic, link retrieved on 16 July 2024.
[37] LuStat, Freight Traffic, link retrieved on 16 July 2024.

- **Inland waterway freight:** the port in Mertert has a total surface of 65 hectares and is specialised in the transportation of heavy materials such as oil, agrifood and construction materials[38]. In 2023, 247 080 tons were exported (with almost 52% being steel products) and 542 193 tons were imported (with almost 70% being fuels/petrol products)[39].
- **Road connectivity:** Luxembourg is located in the centre of Western Europe and is a member of the Schengen Area. All major transport hubs (cf. above) are located directly at the road network from which the major European highways and major European cities are easily accessible[40].

**International business: partner countries**

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 and 2023. 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[41], which underlines the importance of Luxembourg as a key hub for structuring cross-border investments and financial services. Nonetheless, it should be noted that the usage of those Special Purpose Entities in Luxembourg has gradually declined over the past few years[42].

**Table 3: Net year-ending FDI position of Luxembourg by partner (in millions of EUR), 2021-2023[43]**

| Year | Outward FDI | Inward FDI | Net FDI |
|---|---|---|---|
| 2021 | 3 919 022,2 | 3 113 984,1 | 805 038,1 |
| 2022 | 3 746 404,7 | 2 825 645,9 | 920 758,8 |
| 2023 | 3 512 875,5 | 2 592 596,3 | 920 279,2 |

Both Luxembourg's outward and inward FDI stocks were somewhat concentrated and top-ten countries accounted for about 75% to 80% of total stocks between 2021 and 2023.

The following table lists top-ten inward FDI countries.

[38] Single Window for Logistics, Logistics infrastructure, link retrieved on 16 July 2024.

[39] LUStat, Activities of the Port Mertert (in tons), link retrieved on 22 January 2025.

[40] Single Window for Logistics, European Road Connectivity, link retrieved on 17 July 2024.

[41] Eurostat, Foreign direct investment – stocks, link.

[42] Eurostat, EU direct investment positions by country, ultimate and immediate counterpart and economic activity (BPM6), link retrieved on 6 February 2025.

[43] 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 (2021 and 2022 retrieved in September 2024 and 2023 data in February 2025).

**Table 4: FDI position (inward stock) by top-ten partner (in millions of EUR), 2021-2023[43]**

| Partner country | 2021 | 2022 | 2023 | 2021-2023 total share |
|---|---|---|---|---|
| United States of America | 820 715,1 | 765 789,8 | 563 558 | 25,2% |
| United Kingdom | 397 263,8 | 267 765,2 | 265 847,2 | 10,9% |
| Netherlands | 246 893,1 | 237 920,9 | 181 157,2 | 7,8% |
| Cayman Islands | 164 037,1 | 178 269,8 | 219 959,4 | 6,6% |
| Ireland | 210 519,7 | 160 915,9 | 159 566 | 6,2% |
| Canada | 135 355,2 | 144 125,7 | 142 733,7 | 5% |
| Germany | 135 409,6 | 124 131,2 | 144 003,7 | 4,7% |
| Belgium | 133 042,2 | 122 656,4 | 127 469,6 | 4,5% |
| Bermuda | 132 996,7 | 137 755,7 | 62 431 | 3,9% |
| British Virgin Islands | 86 050,2 | 89 218,4 | 90 881,8 | 3,1% |

All European countries (including the United Kingdom) accounted for around 40% of Luxembourg's inward investments. In addition, the United States of America alone represented about 25% of the inward investment stock in 2021 and 2023, as shown in Table 4.

The following table lists top-ten outward FDI countries.

**Table 5: FDI position (outward stock) by top-ten partner (in millions of EUR), 2021-2023[43]**

| Partner country | 2021 | 2022 | 2023 | 2021-2023 total share |
|---|---|---|---|---|
| United States of America | 588 879,9 | 615 588,8 | 576 406,5 | 15,94% |
| United Kingdom | 687 066,0 | 459 457,2 | 464 352,7 | 14,42% |
| Netherlands | 515 779,7 | 455 645,1 | 415 043,9 | 12,41% |
| Switzerland | 327 766,8 | 328 577,2 | 274 397,1 | 8,33% |
| Germany | 247 967,7 | 200 158,2 | 224 456,2 | 6,02% |
| Ireland | 240 253,8 | 222 404,3 | 130 458,2 | 5,31% |
| France | 159 754,7 | 176 928,0 | 184 460,6 | 4,67% |
| Belgium | 125 543,1 | 139 502,4 | 135 299,7 | 3,58% |
| Spain | 92 879,3 | 118 651,3 | 120 284,7 | 2,97% |
| Cyprus | 94 763,3 | 92 821,8 | 96 128,4 | 2,59% |

On the other hand, Luxembourg's outward FDI was concentrated towards European countries. The United States of America accounted for another 16% of the stock, as shown in the table above.

**Insight Box 1: ML risks Luxembourg FDI countries**

**Risk and context – FATF mutual evaluation reports (4th round)**

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 2021-2022 period, were studied.

All studied partner countries have been assessed to have effective AML/CFT regimes in place and provide good international cooperation. Fraud and drug trafficking are cited in all these FATF mutual evaluation reports as a key threat, followed by organised crime and human trafficking. The abuse of legal persons is also mentioned in all analysed reports as a key vulnerability.

# 4. Methodology

This National Risk Assessment (NRA) was conducted by the MoJ using a structured and rigorous approach. The methodology used in the NRA was developed having regard to the methodologies developed by other jurisdictions, international guidance (e.g. FATF's guidance, the EU's anti-money laundering directives, EU SNRA, EBA opinion and reports), the World Bank and IMF approaches, and extensive consultation with public and private sector stakeholders. The approach combines qualitative and quantitative information and professional expertise.

The NRA exercise takes a national perspective (i.e. it is based on the macro-level analysis described in the section 4.2 further below) to contribute to the understanding of ML risks at a country and sector level. The assessment focuses mostly on supervisory authorities, self-regulatory bodies (SRBs), the financial intelligence unit, law enforcement agencies and cross-agency committees, where applicable. The methodology also leverages outputs and insights from meso-level and micro-level analyses for collecting more granular inputs and data and enhance the macro-level view.

Ahead of describing the approach in detail, the following definitions are introduced:

**Table 6: Methodology – Key definitions[44]**

| Term | Definition |
|---|---|
| **Threat** | A threat, in general, is a person, group or activity with the potential to cause harm to the state, society or the economy. In the ML context this refers to criminal individuals, groups or entities and their facilitators seeking to conceal the illicit origins of funds through past, present and future ML activities (and not the predicate offences themselves). |
| **Vulnerability** | A vulnerability can be exploited by the threat or may support or facilitate its activities. In the ML risk assessment context, looking at vulnerabilities as being distinct from threats means focusing on, for example, the inherent features of a particular sector, a financial product or type of service that makes them attractive and feasible for ML purposes. Certain inherent characteristics of a country can also make it vulnerable to ML including a large financial, trade, or company formation sector. Vulnerabilities may also relate to a weakness in law, regulation, supervision, or enforcement. |
| **Consequence** | A consequence refers to the impact or harm that ML may cause and includes the effect of the underlying criminal activity on financial systems and institutions, as well as the economy and society at large. These consequences can be both domestic and international in scope, reflecting the far-reaching nature of ML activities. The consequences of ML may be short or long term in nature and relate to harm to populations, specific communities, the business environment and national or |

[44] FATF, *Money Laundering National Risk Assessment Guidance 2024,* link.

| Term | Definition |
|---|---|
| | international interests. It can also undermine the reputation and attractiveness of a country's financial sector. |
| **Risk** | Function of three factors: threat, vulnerability and consequence. |
| **Inherent risk** | Inherent risk is the extent of risk present without the consideration of any risk mitigation measures. |
| **Mitigating factor** | Risk mitigating factors are actions, controls or strategies implemented to manage the identified ML risks. Risk mitigating measures can include legislative, regulatory, supervisory, law enforcement, or other administrative actions taken to mitigate risks within the national AML framework. |
| **Residual risk** | Residual risk takes into account the impact of a country's mitigation measures. |

## 4.1. Process and stakeholders

The NRA exercise is conducted in two steps:

- the inherent risk assessment, encompassing the analysis of threats and vulnerabilities; and
- the residual risk assessment, encompassing the analysis of mitigating factors in place.

The findings of the inherent risks and the impact of mitigating factors as well as the outcomes in residual risks are consolidated and jointly assessed. They constitute a key element to develop the national multi-annual AML/CFT Strategy.

The NRA exercise involves defining the scope, granularity and approach up front, collating relevant national and international data and information, reviewing and refining hypotheses developed using expert opinion, iterating intermediate outputs with the relevant experts, and agreeing final outputs, outcomes and improvement measures resulting from the assessment.

At all three steps of the NRA exercise, multiple public and private stakeholders were 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 and Diekirch District Court
- Judicial Police Service (SPJ)[45]
- Prosecution authorities:
    - General State Prosecutor's Office
    - State Prosecutor's Offices of the Luxembourg and Diekirch District Courts
- Asset management and asset recovery authorities:
    - Asset Management Office (AMO)
    - Asset Recovery Office (ARO)
- Others:
    - Luxembourg Business Registers (LBR)
    - Luxembourg Central Bank (BCL)
    - European Public Prosecutor's Office (EPPO)

For the inherent risk assessment, different stakeholders were engaged for the threat and the vulnerabilities assessment. For the threat assessment, the analyses were performed together with the prosecution authorities and the CRF, with additional inputs from other agencies. The vulnerabilities assessment primarily involved supervisors and SRBs as stakeholders, with additional information collected from other agencies, such as the LBR.

The threat and vulnerabilities assessments followed similar stakeholder engagement processes. First, 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 or vulnerability status in Luxembourg, identify additional data points to be collected and validate hypotheses on the levels of risk. Following the data and input collection, findings were summarised in an NRA text narrative and scorecards (further detailed in sub-sections below). They were reviewed by the stakeholders via written communication and additional bilateral meetings. This process allowed for increasingly granular analyses, with follow-up communications typically focusing on higher-risk areas.

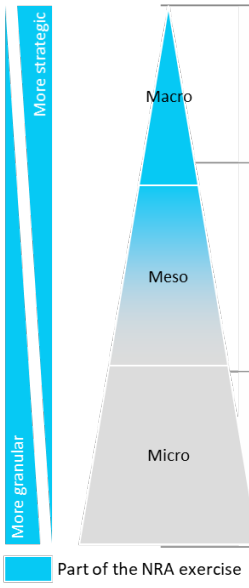
[45] The SPJ is the department within the Grand-Ducal Police (PGD) in charge of executing most orders from the State Prosecutors and the investigative judges.

To understand the impact of mitigating factors on inherent risks, stakeholders specified above were involved. Similar to the inherent risk assessments, data requests were first sent to supervisors, SRBs and prosecution authorities, and customised data requests were sent to multiple stakeholders. Bilateral meetings were used to collect expert insights from stakeholders, identify areas for further analyses and additional data collection, and validate the outcomes of the analyses. The NRA text narratives and scorecards were iterated with the appropriate stakeholders to identify specific areas for further analyses and validate the final versions of them.

## 4.2. Granularity and scope of the NRA

The figure below illustrates and explains the different levels of granularity of different risk assessment types and links them to the "scope" of the NRA exercise.

**Figure 3: Different levels of granularity of risk assessments**




| | Level of analysis | Type of assessment | Objective | Data used | Relevance for NRA |
|---|---|---|---|---|---|
| Macro | **Macro analysis** (i.e. sector-level, threat-level) – top-down | • EU Supra-National Risk Assessment<br>• National Risk Assessment | • ML/TF overall strategy<br>• Resource allocation across supervisors<br>• Prioritisation within cross-cutting agencies (e.g. FIU, justice, law enforcement) | • Macro-economic/ Financial data<br>• General crime data<br>• Demographic/ Census data | • Focus of NRA |
| Meso | **Meso analysis** bridging macro- and micro-analysis | • Vertical risk assessments (e.g. Terrorism Financing)<br>• Sub-sector risk assessments (e.g. Private banking) | • Sector-specific strategy<br>• Prioritisation within supervisors<br>• Sector-specific rules (e.g. enhanced CDD) | • Aggregated micro-data<br>• Surveys/Questionnaires<br>• Expert judgement<br>• National data on sub-sectors & predicate offences | • Use mid-level data where possible (e.g. questionnaires of supervisors)<br>• Integrate sub-sector and vertical risk assessments |
| Micro | **Micro analysis** (at product, crime, entity level) | • Entity-level risk assessments (and detailed assessments on threats or products) | • Product-specific rules<br>• Supervisor actions (e.g. examinations)<br>• Focused approach to tackling high risk crimes | • Granular data on:<br>• Products<br>• Crimes (e.g. case studies)<br>• Entities<br>• Legal features | • N/A |

Part of the NRA exercise

At the top, the macro-level analysis provides a high-level view of the main ML threats and vulnerabilities and thus supports the strategy determination and resource allocation at the national level across different supervisory, detection and prosecution agencies. This analysis assesses Luxembourg's ML risk at the level of predicate offences for threats (e.g. drug trafficking, fraud and counterfeiting) and at the sector-level for vulnerabilities (e.g. banking and insurance). The objective of this assessment is to compare ML exposure across threats and sectors to inform overall strategy and enable resource prioritisation.

The meso-level analysis is a mid-level risk assessment which is used as input for the macro-level analysis by providing more granular data and inputs. It uses aggregated micro-level data where applicable (e.g. reports on the insurance sector), national surveys/questionnaire findings and agency expert opinion. The objective is to inform sector-specific strategy and enable resource prioritisation within supervisors and LEAs.

Data inputs to the meso-level analyses include quantitative data and qualitative information gathered from national data sources (some public, some confidential), and from agencies themselves (e.g. aggregating information from AML/CFT questionnaires) along the dimensions of the assessment criteria. For instance, the size of the retail and business banking sub-sectors use data representing value of customer deposits by type and assets.

Multiple Luxembourg competent authorities have independently conducted meso-level analyses in the form of sub-sector risk assessments. The published versions of those risk assessments are used as inputs for the NRA: for example, the CSSF's risk assessments on private banking[46] and collective investments funds[47]. The sub-sector risk assessments include granular product or segment taxonomies within an analysed sub-sector, exposure to threats and subsequent vulnerability assessments. The risk assessments also include high-level descriptions of existing mitigating factors put in place both by the public and the private sector.

The micro-level analysis is a detailed risk assessment wherein sectorial inherent risk is assessed at the product, service, entity and technical levels, etc. (e.g. current accounts within retail banking most commonly used for ML) and threats are analysed at a granular crime level (e.g. different types of fraud across VAT fraud, online payment fraud, and their usage for ML). For example, supervisors use entity-level risk assessments to determine the entities for which further supervisory off-site measures and on-site inspections will be performed. The objective of this assessment is to inform supervisory actions and identify specific entities/products which are higher risk.

This NRA focuses primarily on the macro- and meso-analyses insofar as they contribute to the multi-annual national AML/CFT strategy. The micro-analysis is not a focus of this exercise, as this is addressed by the routine supervisory and intelligence analyses. Moreover, the micro-analysis is for internal use of supervisors, intelligence and/or LEAs only.

## 4.3. Scorecard approach

The inherent and residual risk assessment leverage a scorecard approach. As such, there is a separate scorecard for the threat assessment, vulnerabilities assessments and the mitigating factors.

The three assessments include the following steps, adjusted for their specificities, which are described in the respective sections below.

First, the taxonomy and the assessment criteria of the analysis are defined. For example, for the threat assessment, the taxonomy covers the predicate offences in Luxembourg, and for the vulnerabilities assessment, it includes the relevant sectors and sub-sectors. The assessment criteria for the threats, vulnerabilities and mitigating factors are defined, together with a rating scale. For example, for the vulnerabilities assessment, criteria include exposure to high-risk geographies or risk profiles of clients.

Second, available data and information are collected against each criterion, which is used to form an understanding of the existing levels of threats, vulnerability or mitigation. The collected data and

[46] CSSF, Private Banking ML/TF Sub-Sector Risk Assessment – 2023 update, link.
[47] CSSF, Collective Investment Sector ML/TF Sub-Sector Risk Assessment – 2022 update, link; 2025 update, link.

information are transformed into a rating against each criterion, which were formalised in the previous step. During this stage, analyses and findings are drafted into an NRA text narrative.

Third and final, the results of the analyses in the second step are aggregated to form a conclusion regarding the overall threat level, a sector's overall vulnerability or the combined effectiveness of mitigating factors. The analyses are also finalised in text narratives, which are presented in separate sections in the NRA below.

## 4.4. Inputs used

This sub-section describes in detail what data and information were used to conduct the NRA. The sources of data and information leveraged can be broadly categorised into five groups: quantitative data from stakeholders, publicly available quantitative data, documents describing mitigating factors, expert inputs and judgement from stakeholders, case studies and typologies.

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 different 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-risk factors.

Publicly available quantitative data included both international and domestically available data sets. For example, international datasets from various sources were used, such as international institutions (UNODC, OECD, European Commission, European Central Bank, Eurostat), and academia (including Organised Crime Portfolio). Domestic data sources were used to complete international data sets (e.g. data provided by *Parquet Général Statistical Service*, CRF Annual Reports, Grand-Ducal Police Annual Reports, STATEC datasets, BCL datasets, data from LBR).

Documents describing mitigating factors were provided by stakeholders for the mitigating factors section in the NRA. Those documents included internal memoranda, describing AML/CFT supervisory frameworks, risk assessment policies, and other internal processes. Agencies also provided information on published circulars, guidance, FAQs and other published materials.

Expert inputs and judgements were used to enhance the analyses of threats, vulnerabilities and mitigating factors. For the threats assessment, interviews and dedicated workshops were used to receive expert inputs on high-risk predicate offences, understand any developments and determine where additional data was 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.

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 ML drivers of sub-sectors observed globally; and Luxembourg stakeholders provided anonymised case studies on previously observed suspicious behaviour by supervised entities or their clients.

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.

## 4.5. Methodology for the threats assessment

Threats are analysed within the inherent risk assessment component of the NRA; that is, in the absence of mitigating factors and controls for ML.

Fundamentally, a threat analysis aims to identify the main proceeds-generating offences that a country's systems are exposed to (i.e. predicate offences, both domestic and international) as well as the criminals perpetuating these offences (i.e. the perpetrators)[48]. Ultimately, the objective of the analysis of threats is to understand the environment in which predicate offences are committed to identify their nature and to assess the exposure to them. The threats assessment is conducted in three different steps:

1. Taxonomy of predicate offences to analyse and criteria for scorecard are defined;
2. Data and expert input are gathered for each criterion/offence to understand the threat level; and
3. Findings are summarized in the NRA text.

In terms of granularity for analysis, threats are assessed along a list of predicate offences in line with FATF crime categories[49]; these map to granular predicate offences (*"infraction primaires"*) under Luxembourg law. Minor adaptations are made to better reflect Luxembourg's reality (for instance, merging "fraud" and "forgery"). A list of predicate offences as defined by the Luxembourg Penal Code is included in Appendix A. The exposure to these threats is considered separately for domestic and external offences. Although terrorism and TF are also predicate offences to ML, a dedicated risk assessment covers risks relating to TF.

Similar to the 2020 NRA, three different criteria are considered to assess the exposure to the threats:

- The "likelihood" criterion assesses the level of criminality (e.g. crime rate, number of offences and convictions).
- The "size" criterion assesses an estimate of the proceeds generated (e.g. amounts seized, value generated, number of STRs) and of the complexity and characteristics of the laundering, i.e. form of proceeds (e.g. cash versus non-cash), ML expertise of criminals and geography (origin / destination).
- The "consequences" criterion helps to distinguish the extent of different threats on financial systems and institutions, as well as the economy and society more generally (i.e. human, social and reputational impact). This is used for domestic, but not for external offences.

[48] FATF, *Money Laundering National Risk Assessment Guidance 2024,* link.
[49] FATF, *NRA Guidance,* 2013, Annex I, link.

**Figure 4: Overview of threat assessment criteria**

| Criteria | Sub-criteria | Example of indicators that can be used |
|---|---|---|
| **Probability of crime** ("likelihood") | Level of criminality | • Crime rate/number of crimes (domestic)<br>• Number of offences, open notices, prosecutions, convictions and sanctions (with and without ML)<br>• MLA & extradiction requests sent and received |
| **Proceeds of crime** ("size") | Proceeds generated | • Number of seizures and amounts seized<br>• Estimated value generated per crime committed<br>• Estimate of trade and financial flows with foreign countries (in particular with high risk countries)<br>• Estimated value of proceeds from international crimes<br>• Number of STRs and SARs filed |
| | Form of proceeds | • Cash proceeds vs. Non-cash physical<br>• Use of innovative forms (e.g. virtual currencies) |
| | ML expertise | • Sophistication (knowledge, skills, expertise)<br>• Capability (network, resources, etc.) |
| | Geography | • Origin/source<br>• Destination |
| **Human, social and reputational impact** ("consequences") | Economic and social cost | • Foregone revenues<br>• Financial system stability and its perceived integrity<br>• Attractiveness of the country for business, ability to attract FDI, broad "reputation" of country |
| | Human harm | • Direct harm to people (injuries, fatalities)<br>• Social harm (e.g. fear of terror, reduced social cohesion) |

**Evaluation**

- Data will be collected to support assessment as much as possible
  - Availability and granularity will differ per crime and criteria (e.g. reputation impacts vs. number of domestic crimes)
  - Often the relative order of magnitude matters most (e.g. corruption index showing Lux as more/less corrupt than others)
- Flexibility in assessment is needed given crimes' differing nature and materiality
  - Not all will have the same level and granularity of data
  - Not all criteria will be equally relevant to all crimes
  - Some crimes will merit more time/data/judgement for assessment vs. Others based on materiality, in line with risk-based approach
  - Assigning a threat level (very low to very high) to each crime will thus be based on a mix of information that was possible to collect (data, rankings, indices, surveys, etc.) and expert judgement


ML threats are assessed on a scale ranging from "Very Low" to "Very High". The following assessment considers both the level of the external and the domestic threat of ML, along the list of predicate offences.

- The external threat corresponds to the threat that foreign proceeds of crime are laundered in Luxembourg (i.e. proceeds of crime committed outside of Luxembourg). The overall risk level of the foreign threat is the function of two factors with equal weight: the likelihood/probability of the threat and the size/proceeds of the threat.
- The domestic threat corresponds to the threat that proceeds from predicate offences committed in Luxembourg are laundered in Luxembourg or abroad. The overall risk level of the domestic threat is the function of three factors with equal weight: the likelihood/probability of the threat, the size/proceeds of the threat, plus the consequences of the threat.

Finally, it should be noted that this assessment is based on existing, publicly available information, confidential information and expert input. As availability and granularity of data per crime varies and considering the number of stakeholders involved in this evaluation process (and all located at different points within the enforcement and penal chain), the associated threat level is a combination of quantitative and qualitative information. The assessment does, therefore, not follow a strict scientific approach, nor is it aiming for a scientific substantiation of results.

Given Luxembourg's open economy and large financial sector, the country is more exposed to ML offences committed by criminals abroad than domestically. Consequently, the national exposure to each threat is calculated as a weighted average between domestic and external exposure, with 25% and 75% weights respectively. For simplicity, the weighting is assumed to be constant across predicate offences. The resulting assessment is described in the threats assessment section of this NRA.

## 4.6. Methodology for the vulnerabilities assessment

For the (sub-)sector vulnerabilities a similar three-step approach is utilised as for the threat assessment:

1. Sectors and sub-sectors subject to the analysis and risk assessment criteria are defined;
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.

The vulnerabilities assessment involves sectors not mapped based on activity but based on supervisory set-up[50]. The detailed mapping tables for the analysed sectors are outlined in section 6.

The criteria used in the scorecard for sectorial vulnerabilities include six dimensions and nine sub-dimensions:

- Structure (consisting of size and fragmentation/complexity);
- Ownership and legal structure;
- Products and activities;
- Geography (consisting of international business and flows with weak AML/CFT measures geographies);
- Client and transactions (consisting of volume and risk); and
- Channels.

Quantitative data and qualitative information are gathered from national data sources (some public, some confidential) along the dimensions of the assessment criteria. The data and information gathered 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 ML). Where data was missing, expert opinion is used to enrich the analysis. The criteria scorecard for the inherent risk scores, together with examples of indicators and data used can be found in Appendix B.

The aggregate inherent risk score across each sub-sector/crime 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 the Appendix B. 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.

[50] This is based on the legal framework of the supervisory set-up with authorities.

## 4.7. Methodology for mitigating factors and residual risk

### *4.7.1. Methodology for impact of mitigating factors*

Following the inherent risk assessment, impact of mitigating factors is assessed. An effective system is one that "properly identifies, assesses and understands its money laundering and terrorist financing risks. […] A country also co-operates and co-ordinates domestically to develop AML/CFT policies"[51]. The aim of this part of the NRA is to establish an accurate, factual picture of the results and the effectiveness of the current AML/CFT framework to mitigate inherent ML risk and set up relevant institutions and identify improvement measures.

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;
3. Aggregation of ratings into a sub-sector rating and translation of findings in NRA text narrative.

To assess the impact of mitigating factors, current practices are discussed with concerned entities along a common set of four dimensions: mandate, model, capabilities, and results. This intended to cover the full lifecycle of supervision, detection and enforcement: authorisation to act by relevant governmental bodies (mandate), set-up (model), resource inputs (capabilities) and outputs (results). The results/effectiveness dimensions are then used to inform the scorecard criteria, which include five different criteria and nine sub-dimensions:

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

Please note that for the purpose of this NRA, the assessment focuses on vulnerabilities and mitigating factors related to ML. Nonetheless, preventive measures, supervisory actions or enforcement measures may tackle ML and TF simultaneously.

The different criteria together with the relevant associated data and information input examples are described in Appendix B.

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

### *4.7.2. Methodology for residual risks*

The residual risk assessment considers the level of ML risk after the implementation of mitigating measures. The residual risk outcomes are used to identify sectors where Luxembourg remains most exposed to ML risks. It thus serves as a basis to develop and prioritise strategic actions that can be undertaken to further strengthen Luxembourg's AML/CFT regime and reduce ML risks. Similar to the assessment of the sectorial inherent risk, the residual risk is developed in conjunction with the concerned authorities.

The inherent risk scores are determined using the scorecard approach described in the sub-section above on a scale from 1 to 5, ranging from "Very Low" risk to "Very High" risk. The scorecard dimensions for sectorial vulnerabilities include size of the sub-sector, fragmentation of the market, ownership/legal structure of the entities, products/activities, client/transaction volumes, client/transaction risks, geographies and international business as well as channels. Scorecards of inherent risk criteria are provided in Appendix B.

Likewise, the mitigating factors impact scores are calculated using the scorecard approach. It takes into account criteria such as market entry controls, understanding of ML risks in the sector, rules setting and rules enforcement by the supervisors and detection and prosecution statistics. These criteria are also provided in Appendix B.

As with the inherent risk assessment, a combination of research, data, expert judgement and bilateral discussions with concerned entities is used to assess the impact of the mitigating factors in place along each of the criteria in the scorecard, on a scale from 1 to 5. Luxembourg-specific data is collected from a wide range of sources such as annual reports (e.g. CSSF, CRF, CAA), statistics (e.g. STATEC) and non-publicly available data from agencies. When data is missing, the assessment is based on expert judgment which is formed through agency interactions. As with inherent risk, a lack of detailed statistics increases the risk assessment in line with a conservative approach.

An overall score on the mitigating factors in place is obtained by averaging the scores across the criteria and "bucketing" these in 5 possible outcomes: an average score of 1 stands for an outcome of "limited or no mitigating factors in place"; an average score of 2 stands for "some mitigating factors in place"; 3 stands for "significant mitigating factors in place"; 4 for "high mitigating factors in place" and 5 for "very high mitigating factors in place". The aggregated outcomes for mitigating factors correspond to a reduction in inherent risk of 0, -0,5, -1, -1,5 and -2, respectively.

Finally, the residual risk score is assessed by taking the inherent risk score (1 to 5) and subtracting the mitigating factors outcome (i.e. reducing the score by 0, 0,5, 1, 1,5 or 2 points). This results in a residual risk score per sub-sector. An illustration of the residual risk calculation, together with an illustrative example, is provided in Appendix B.

# 5. Inherent risk – threats assessment

An overview of the ML threat level per category – including a breakdown per predicate offence – is provided in the table below. Threats have been assessed along a list of predicate offences in line with FATF crime categories; these map to granular predicate offences under Luxembourg law. A full mapping table is provided in Appendix A. The overall threat assessment is based on a weighted average between external and domestic exposure, with 75% and 25% weights respectively. Given Luxembourg's open economy and large financial sector, the country is more exposed to ML from criminals abroad than domestically. For simplicity, the weighting is assumed to be constant across predicate offences. The rest of this section provides a more detailed assessment per crime category, split into external and domestic exposure to ML.

**Table 7: Threats assessment, weighted average exposure**

| Predicate offence | External threat level (75%) | Domestic threat level (25%) | Weighted average exposure |
|---|---|---|---|
| Fraud and forgery | Very High | High | Very High |
| Tax crimes | Very High | Medium | Very High |
| Corruption and bribery | Very High | Medium | Very High |
| Drug trafficking | High | High | High |
| Participation in an organised criminal group and racketeering | High | Medium | High |
| Sexual exploitation, including sexual exploitation of children | High | Medium | High |
| Cybercrime | High | Medium | High |
| Counterfeiting and piracy of products | High | Low | High |
| Smuggling | Medium | Low | Medium |
| Insider trading and market manipulation | Medium | Low | Medium |
| Robbery and theft | Medium | High | Medium |
| Trafficking in human beings and migrant smuggling | Medium | Medium | Medium |
| Illicit trafficking in stolen and other goods | Medium | Low | Medium |
| Extortion | Low | Low | Low |
| Illicit arms trafficking | Low | Low | Low |
| Environmental crime | Low | Low | Low |
| Murder and grievous bodily injury | Low | Low | Low |
| Kidnapping, illegal restraint and hostage taking | Low | Low | Low |
| Counterfeiting currency | Low | Very Low | Very Low |
| Piracy | Low | Very Low | Very Low |

## 5.1. External exposure: money laundering of proceeds of foreign crimes

Given its position as a financial centre and the low level of local criminality, ML of proceeds of foreign crimes is the most significant ML threat for Luxembourg. The magnitude, cross-border character and the diversity of funds and transactions being handled by Luxembourg's (non-)financial sectors contribute to this exposure. In a similar vein, and considering the limited size of the domestic market, Luxembourg's economy is internationally oriented with a significant share of businesses receiving and disbursing funds abroad (cf. section 3).

ML of foreign crimes accounts for a significant share of mutual legal assistance (MLA) requests[52]. Across all crimes, the prosecution authorities received over 2 700 MLA requests requiring coercive measures and almost 4 000 MLAs requiring non-coercive measures on aggregate between 2020 and 2023. Those related to ML amounted to around 600 (with around 400 ML requests and around 200 additional MLA requests).

The following table summarises the level of likelihood/probability, size/proceeds and overall external threat level for every ML-related predicate offence.

**Table 8: External threat level overview**

| Predicate offence | Likelihood/ probability | Size/ proceeds | External threat level |
|---|---|---|---|
| Fraud and forgery | Very High | Very High | Very High |
| Tax crimes | Very High | Very High | Very High |
| Corruption and bribery | High | Very High | Very High |
| Drug trafficking | High | High | High |
| Participation in an organised criminal group and racketeering | Medium | Very High | High |
| Sexual exploitation, including sexual exploitation of children | High | Medium | High |
| Cybercrime | High | Medium | High |
| Counterfeiting and piracy of products | High | Medium | High |
| Smuggling | Medium | Medium | Medium |
| Insider trading and market manipulation | Medium | Medium | Medium |
| Robbery and theft | Medium | Medium | Medium |
| Trafficking in human beings and migrant smuggling | Medium | Medium | Medium |
| Illicit trafficking in stolen and other goods | Medium | Medium | Medium |
| Extortion | Low | Low | Low |
| Illicit arms trafficking | Low | Low | Low |
| Environmental crime | Low | Low | Low |
| Murder and grievous bodily injury | Low | Low | Low |
| Kidnapping, illegal restraint and hostage taking | Low | Low | Low |
| Counterfeiting currency | Low | Low | Low |
| Piracy | Low | Low | Low |

[52] *Parquet Général* Statistical Service.

### *5.1.1. Fraud and forgery*

| Please note that this section should be read in conjunction with sections 5.1.5, 5.1.8, and 5.2.1. |
|---|

A wide range of different categories of illicit activities fall within the scope of fraud and forgery (see Appendix A). Nevertheless, the following two sub-sections will elaborate on two relevant topics. The first tackles cyber-enabled fraud (CEF), a phenomenon that has rapidly evolved over the past few years. A second sub-section addresses fraud affecting the EU's financial interests, considering that the EPPO became operational on 1 June 2021, and given that the EPPO has its headquarters and is operating in Luxembourg.

#### *5.1.1.1. Cyber-enabled fraud*

Pursuant to the FATF-Interpol-Egmont Group, CEF has increased significantly in recent years[53]. Although there is no complete estimate of the global magnitude and scale of CEF, its consistent growth has generally been acknowledged in the past few years[54].

CEF can take many different forms, but it generally refers to fraud that is enabled through or conducted in the cyber environment and that involves (i) transnational criminality such as transnational actors and funds flows and (ii) deceptive social engineering techniques (i.e., manipulating victims to obtain access to confidential or personal information). CEF and related ML are often executed by transnational organised criminal groups or syndicates[55].

Digitalisation and the development of new technologies serve as key drivers underpinning the scale, scope and speed of CEF. Technical innovation and the continuing digital transformation have led to a significant evolution of the payments industry over recent years. As a result, more citizens (including vulnerable groups) are participating in online activity. At the same time, digitalisation means jurisdictions are becoming increasingly connected with information and funds moving swiftly across borders. These factors have fundamentally altered the criminal landscape and created an environment of increased threats from CEF. Generated proceeds are rapidly laundered through a network of accounts. These networks typically involve individuals as well as legal entities[56]:

- Individual money mules may be recruited by criminals via various means, including through job offers and advertisements, as well as online social media interactions. Money mules may be knowingly complicit in the laundering of funds or work unwittingly (through deception), or negligently, and may also be offered incentives or fees to handle the illicit funds.
- Shell companies are under the control of CEF criminals, and typically have recourse to strawmen or nominee directors. Individual money mules recruited may also be instructed to act as such strawmen, and open corporate accounts in a bid to further obscure criminal ownership.

[53] The term cyber-enabled fraud covers: business email compromise, phishing fraud, social media and telecommunication impersonation fraud, online trading, online romance fraud, employment scams.
[54] FATF – Interpol - Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud*, 2023, link.
[55] FATF – Interpol - Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud*, 2023, link.
[56] FATF – Interpol - Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud*, 2023, link.

- Legitimate companies, similar to individual money mules, may also be tricked into receiving CEF-proceeds (e.g. as an investment or business opportunity) and asked to either re-direct the funds or be refunded into a separate criminally controlled account. In some cases, legitimate companies were observed to willingly accept such "business opportunities" particularly in times of economic distress. The involvement of legitimate companies provides an additional façade to mask illicit activities from detection.

Usually, CEF related proceeds can be laundered quickly through a network of accounts, which often span across multiple jurisdictions and FIs. To layer the proceeds of crime, criminals were observed to use cash withdrawals in order to transport the funds cross-border and to reinject the funds by using trade-based ML techniques (e.g. fictitious or false invoicing)[57].

The use of crypto assets, especially with regard to investment fraud, has become more prevalent. Factors such as the increase in value of certain crypto assets and growing media attention around crypto investments are also contributing factors to the steady surge in investment fraud cases. With respect to investment fraud, Europol notes that Bitcoins are increasingly being converted to stable coins, most likely because they are less subject to price volatility. The involvement of non-compliant crypto service providers with insufficient levels of KYC in offshore jurisdictions remains one of the main challenges in many cryptocurrency investigations as they often give rise to lengthy MLA procedures[58,59].

As noted earlier, advancements in technology and digitalisation have given rise to the development of new and existing products and services. One of those services are, for instance, virtual IBANS (vIBAN). While vIBANs are used in many different legitimate ways, such as facilitating and categorising payments from multiple parties, the FATF-Egmont report has flagged the abuse of vIBANs as a tool used for CEF-related ML[60]. Moreover, due to the intrinsic characteristics of vIBANs (cf. Insight Box 2), LEAs are faced with difficulties in identifying and tracing of illicit funds transiting through vIBANs.

**Insight Box 2: Virtual IBAN**

**What is a virtual IBAN?**

Virtual International Bank Account numbers, also known as vIBANs are functionally identical to regular IBANs in that they can be used to send and receive payments on a global scale. They are functionally and visually indistinguishable from regular IBANs[61].

Whereas a regular IBAN is directly matched to a bank account (i.e., there is only one single bank account linked to each individual IBAN number), a vIBAN is a virtual number that is not matched to an account in a physical bank. They are bank-issued reference numbers that enable incoming payments to be rerouted to a physical IBAN, which is itself linked to a physical bank account. vIBANs cannot hold any

[57] FATF – Interpol - Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud*, 2023, link.

[58] Europol, *Internet organised crime threat assessment 2024*, link.

[59] "Stablecoin" refers to a type of cryptocurrency where the value of the digital asset is supposed to be linked to a reference asset, which is either fiat money, exchange-traded commodities or another cryptocurrency, making it less subject to price volatility than other types of cryptocurrencies.

[60] FATF – Interpol - Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud*, 2023, link.

[61] FATF – Interpol - Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud*, 2023, link.

funds, and their balance is constantly zero. vIBAN holders can also have several unique vIBANs, which reroute and centralize all payments into a single physical bank account. Furthermore, vIBANs may be issued by FIs without a banking licence (e.g. Payment Service Providers, EMIs)[62].

VIBANs are often used for legitimate purposes, such as for the international management of receivables as payments can be received by geographical zone or currency[63]. They can also be used for reconciliation and record-keeping processes, for example in situations where big utilities companies manage a large number of customers and payments[64]. These FIs and providers can then re-issue the vIBANs to their own clients. If these clients are also FIs and providers of vIBANs, they can again re-issue the vIBANs to their clients.

Since vIBANs are visually identical to conventional IBANs, they can make transaction monitoring and the detection of suspicious transactions difficult for the following reasons:

- vIBANs can be created remotely from any country around the world, and account holders can choose between different country codes when creating a new vIBAN. Thus, it may be challenging to identify where the physical account is located.
- a vIBAN can have multiple intermediaries before arriving at its final client. These multiple intermediaries increase the level of complexity and ambiguity as it might be challenging to identify the "true" issuer[65].

#### *5.1.1.2. Fraud affecting the EU's financial interests – expenditure fraud*

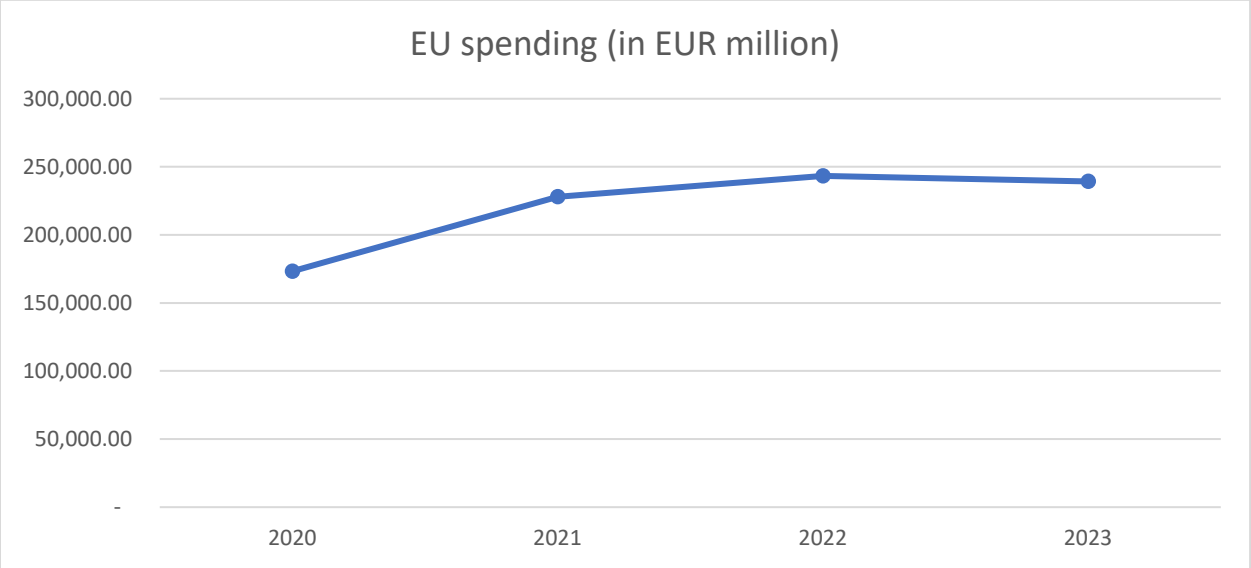
Overall, the EU budget is used to finance EU priorities and projects that most EU Member States could not finance on their own, either because of the project's size or its cross-border nature. The EU adopts long-term spending plans, known as multi-annual financial frameworks[66]. This budget is financed, amongst others, by a proportion of each EU country's gross national income, custom duties and a portion of the VAT collected by each EU country[67].

The current EU 2021-2027 Multiannual Financial Framework (MFF) foresees a spending of EUR 1,211 trillion topped up with an additional EUR 806,9 billion stemming from the NextGenerationEU. These funds are allocated to different programs and public funds, such as the European Agricultural Guarantee Fund (EUR 291 billion) or the European Regional Development Fund (EUR 226 billion)[68].

The following graph depicts the level of EU spending and revenue within the MFF for years 2020 to 2023.

[62] Europol Financial Intelligence Public Private Partnership. A copy of this document can be requested from the CRF by sending a request via goAML.
[63] CTIF-CFI, *Annual report 2021,* link.
[64] EBA, *EBA Report on ML/TF risks affecting the EU's financial sector,* 2023, link.
[65] Europol Financial Intelligence Public Private Partnership. A copy of this document can be requested from the CRF by sending a request via goAML.
[66] European Union, How the EU budget is spent, link retrieved October 2024.
[67] European Union, How the EU budget is financed, link retrieved October 2024.
[68] European Commission, EU spending and revenue 2021-2027, link retrieved October 2024.

**Figure 5: EU budget spending, 2020-2023**[69]




**Insight Box 3: The European Prosecutor's Office (EPPO)**

**European Public Prosecutor's Office (EPPO) – Mission and tasks**

The European Public Prosecutor's Office (EPPO) is the independent prosecution office of the EU. It is responsible for investigating, prosecuting and bringing to judgment crimes against the financial interests of the EU. These include several types of fraud as subsidy fraud, cross-border VAT fraud with damages above EUR 10 million, ML, corruption, etc.

The EPPO undertakes investigations, carries out acts of prosecution and exercises the functions of prosecutor in the competent courts of the participating Member States, until the case has been finally disposed of. Up until the EPPO started its operations, only national authorities could investigate and prosecute these crimes, but their powers stopped at the borders of their country. The EPPO was established to enhance the fight against crimes impacting the financial interests of the Union by addressing inter alia the fragmentation of such national prosecutions. This objective relies on the EPPO's ability to proactively, comprehensively, and efficiently identify connections among ongoing investigations, maintaining a continuous overview of this inherently cross-border form of organised crime. Organisations like Eurojust, OLAF and Europol do not have the necessary powers to carry out such criminal investigations and prosecutions.

**What are the financial interests of the EU?**

[69] EU spending and revenue – Data 2000 – 2023, link retrieved on 20 September 2024.

All revenues, expenditures and assets covered by, acquired through, or due to the EU budget and the budgets of the institutions, bodies, offices and agencies established under the Treaties, and budgets managed and monitored by them[70,71].

By 31 December 2023, the EPPO had 1 927 active investigations for an estimated damage of over EUR 19,2 billion.

The 2023 annual report of the EPPO notes that by the end of 2023, around one third of the offences investigated by the latter concerned alleged non-procurement expenditure fraud. This type of fraud is committed via the use or presentation of false, incorrect or incomplete documents in order to receive funds (financial aid, subsidies) from the EU budget, which they would otherwise not be entitled to. The EPPO detected such type of frauds in sectors such as agriculture, fisheries, infrastructure, regional development, healthcare, social affairs, youth and labor, research and innovation and support for small and medium-sized enterprises (SMEs). Recovery funds related to the consequences of the Covid-19 pandemic, particularly those covered by the European Commission's Recovery and Resilience Facility, were also targeted by fraudsters.

Around 8,5% of the offences investigated by the EPPO by the end of 2023 concerned suspected procurement expenditure fraud, which often consists in unlawfully manipulating tendering procedures for public works, and is predominantly committed via the use or presentation of false, incorrect or incomplete statements or documents. The following sectors were identified as being vulnerable to this type of fraud: agriculture, infrastructure and regional development, education, research and innovation, social affairs and human resources as well as funds related to the Covid-19 pandemic.

The EU Recovery and Resilience Facility (RRF) is the cornerstone of NextGenerationEU, an EU recovery instrument aiming to repair the immediate economic and social damage of the COVID-19 pandemic. The RRF will disburse up to EUR 648 billion (in 2022 prices) in grants and loans to EU Member States. By the end of 2023, the EPPO had 206 active investigations related to NextGenerationEU funding, with an estimated damage of over EUR 1,8 billion. This represents approximately 15% of all the cases of expenditure fraud handled by the EPPO in 2023, but in terms of estimated damage, it corresponds to almost 25%. This shows that NextGenerationEU funding is a target for fraudster. EPPO's investigations concerned a variety of projects financed under NextGenerationEU: public transport; public infrastructure; the green economy and technology; support to company competiveness; innovation and digital transformation; training and development; education and research; health; and public administration. Investigations into offences related to specific programmes, such as the 'repair bonus' and the 'energy bonus', designed to support citizens in making environmentally sustainable choices were also opened. In 2023, the main sources of detection and reporting to the EPPO in this area were, by far, national LEAs. Their ability to detect fraud in this area was the strongest when they took a pro-active analytic approach.

[70] EPPO, Mission and task, link retrieved on 30 July 2024.

[71] The Directive (EU) 2017/1371 ("the PIF Directive") defines which crimes are considered crimes affecting the EU budget as well as the notion of "financial interest of the EU".

In several cases (especially those related to NextGenerationEU), the EPPO observed that the frauds were related to funds that had been wired to beneficiaries as an upfront payment, in order to cope with the expenses of the initial phase of a project. In fact, these beneficiaries turned out to be sham companies or fictitious economic operators; the projects were not effectively carried out, and the funds were immediately transferred to bank accounts abroad, with a final destination in non-EU countries[72].

According to the EPPO, the Luxembourg's office handled several assisting measures in expenditure fraud cases investigated in other EPPO Member States.

#### *5.1.1.3. Luxembourg's external threat exposure to fraud and forgery*

With regard to the Luxembourg context, its position as a payments, investment and cyber hub increases the likelihood that criminals (in Luxembourg and abroad) commit fraud involving Luxembourg-based FIs (wittingly or unwittingly) and potentially launder the proceeds of that fraud via Luxembourg.

This is further outlined by the FATF mutual evaluation reports of Luxembourg's key inward investment countries which cite fraud as a key ML threat (cf. Insight Box 1). Considering the significance and extent of these financial flows, some of these might be linked to fraud.

For instance, the Grand-Ducal Police has observed that some PIs established in Luxembourg are misused to transfer funds originating from fraudulent activities to crypto-currency exchange platforms[73].

Between 2020 and 2023, the CRF identified around 79 000 reports with respect to fraud and around 13 000 with regard to forgery. Among these 92 000 reports, about 86 500 were filed by entities operating online[74]. It should be noted that these entities file, in general, the most significant number of reports with the CRF. These entities use effective and highly sophisticated transaction monitoring tools. Besides, numerous of these entities have established their European headquarter in Luxembourg. Consequently, the only link with Luxembourg is the headquartered entity and the Luxembourg account. The CRF disseminates relevant information with their foreign counterparts through international cooperation mechanisms and froze about EUR 55 million[75].

Overall, the judicial authorities and LEAs noted that fraudsters target both natural and legal persons and that the prejudice may be very small or very significant, depending on the type and profile of the targeted person. The following case study illustrates a case of abusing assets of a foreign non-profit organization (NPO):

[72] EPPO, *2023 Annual Report*, link.

[73] Police Grand Ducale, *Rapport d'activités 2023*, link.

[74] Please note that throughout section 5, the definition of "entities operating online" refers to the one included in the CRF's annual reports (section 2.1.2 *prestataires en ligne*) and encompasses PIs, EMIs, VASPs, and banks operating online. The CRF's annual reports can be accessed here: link.

[75] CRF, *Rapport annuel 2021-2022*, link and CRF, *Rapport annuel 2023,* link.

**Case study 1: External threat – fraud/abuse of a foreign NPO's assets**[76]

Suspicions were raised based on various wire transfers observed between a foreign NPO, a Luxembourgish company (hereafter "LuxCo") and the private account of the LuxCo's ultimate beneficial owner (hereafter "Mr. X").

The foreign NPO paid substantial sums to Mr. X's personal bank accounts in Luxembourg and abroad, as well as the LuxCo's corporate bank account. The funds received from the foreign NPO were the LuxCo's sole source of income. Moreover, no apparent link existed between the foreign NPO's activity and the LuxCo's official business purpose according to which the LuxCo should be active in sales, marketing and distribution of various objects and products to professionals.

Furthermore, outgoing payments to accounts of Mr. X's family were identified. The funds were then used for private purposes, as for example the purchase of different real estate properties or cars.

Which was even more serious, was the fact that the inflows of the foreign NPO's Luxembourgish bank account were exclusively donations paid in from foreign debit cards and relating to donations made for sick children. No outgoing transaction in connection with the fulfillment of the foreign NPO's purpose was observed.

Red flags:

- No online presence, website or official listing of the foreign NPO.
- Circular transactions between the ultimate beneficial owner's account, the LuxCo and the foreign NPO.
- No outgoing transactions in line with the NPO's purpose.
- No incoming and outgoing transactions in line with the LuxCo's business purpose.

Judicial authorities received, between 2020 and 2023, over 1 200 MLA requests in relation to fraud and forgery. The Grand-Ducal Police observes that fraud is among the top-five crime area with regard to incoming and outgoing information exchange via Europol's secure information exchange network application.

Considering the above, the overall external threat level is assessed to be "Very High".

### *5.1.2. Tax crimes*

It should be noted that this section should be read in conjunction with sections 5.1.1 and 5.1.5.

Tax crimes relate to both direct tax and indirect tax crimes.

[76] Case study provided by the CRF.

#### *5.1.2.1. Direct taxes*

Overall, there are two main scenarios on how Luxembourg may be exposed to ML from direct tax crimes committed abroad[77]:

- A non-resident natural person may open an account in Luxembourg and place funds non-declared in his/her residence country. Nevertheless, this typology may be less prevalent since the EU adopted the Common Reporting Standards (CRS) for the automatic exchange of information regarding financial accounts between tax authorities. In a similar vein, it should be mentioned that Luxembourg has also signed numerous agreements and Memoranda of Understanding (MoUs) with other countries and international organisations with regard to fiscal matters and exchange of information. A full list of these agreements can be found on the ACD's website;
- A Luxembourg legal person (tax resident) may be misused as part of other arrangements to deceive foreign tax authorities or to avoid that a non-resident person pays taxes in its home country.

The level of tax and banking transparency has significantly increased in recent years[78]. Nonetheless, there is a risk that Luxembourg non-residents continue trying to abuse or misuse Luxembourg FIs and DNFBPs (i.e., lawyers and accountants) to commit tax crimes in their residence country.

As noted above, intra-administrative international cooperation in tax matters is an important mitigating measure to prevent tax crimes. The number of these exchanges (see Insight Box below) and the partner country involved may provide information useful for the assessment of this threat, especially with regard to Luxembourg's financial centre.

**Insight Box 4: EOIR and AEOI**

Both EOIR and AEOI are cross-border information sharing mechanisms for tax purposes between tax administrations.

**Exchange of Information on Request (EOIR)**: Exchanges of tax information on request are carried out by a requesting tax administration that needs information or documents available in the requested country as part of a tax investigation when it has exhausted internal avenues and when the criterion of foreseeable relevance is met. When the administration does not hold the requested information, it sends an injunction request to the holder of the information to transmit it, after receipt, to the requesting country.

**Automatic Exchange of Information (AEOI):** Various international agreements, including Directive 2011/16/EU on administrative cooperation (DAC), as amended, require the ACD to automatically exchange with other partner jurisdictions (EU Member States or OECD countries), namely:

- data relating to certain persons and income (e.g. salaries, pensions, directors' fees) received in Luxembourg by non-residents;

[77] The case of a Luxembourg legal person being misused to commit tax crimes in Luxembourg that may be laundered in Luxembourg or abroad is considered as domestic exposure.

[78] Access to the MoF's thematic dossier presenting Luxembourg's commitment with regard to tax transparency: link.

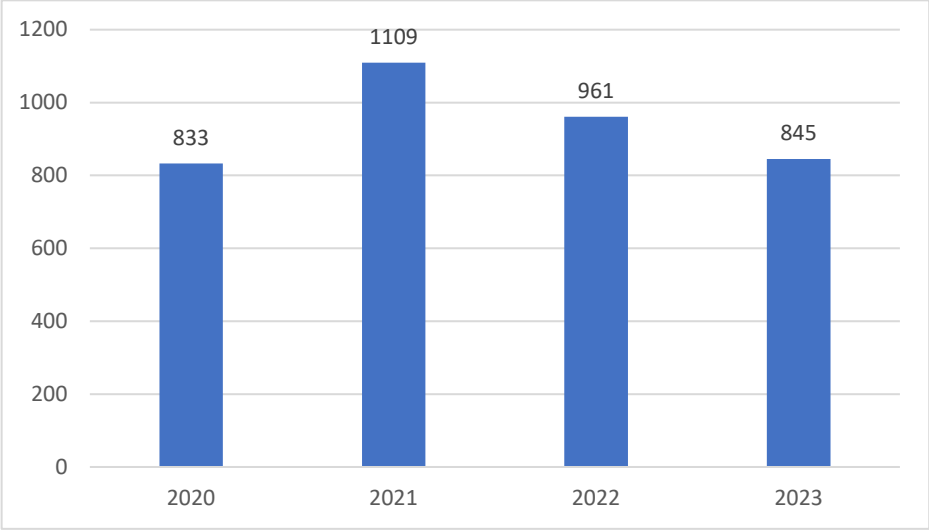
- data relating to financial assets and accounts held in Luxembourg by non-residents;
- country-by-country reports filed by constituent entities in Luxembourg;
- tax rulings;
- cross-border arrangements filed by intermediaries or taxpayers in Luxembourg,
- declarations of platform operators.

In a similar vein, partner jurisdictions must send the ACD, namely data relating to Luxembourg residents and their income or country-by-country reports/tax rulings/cross-border arrangements filed in their jurisdiction. This data is exchanged annually within predefined deadlines through computerized systems.

Considering Luxembourg's position as a transnational financial centre, the number of outgoing AEOI and the number of incoming EOIR exceeds the number of incoming AEOI and outgoing EOIR, except for cross-border arrangements filed by intermediaries or taxpayers where the number of incoming AEOI exceeds the number of outgoing AEOI.

The following two figures evidence the number of EOIR received by the ACD as well as the number of outgoing AEOI sent by the ACD.

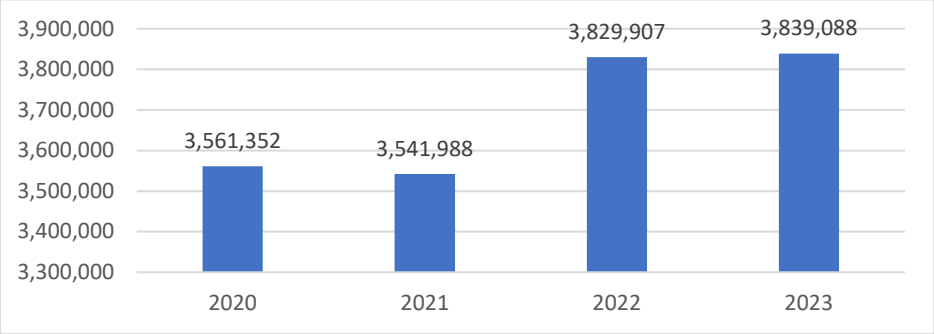
**Figure 6: Incoming requests for tax information (EOIR), 2020 - 2023[79]**




Following the pandemic, the number of EOIR fell in 2020 and 2021 saw a surge in the number of requests (catch-up phenomenon). Overall, about two third of all requests of information related to natural persons and most of them originated from France (about 45% of all EOIR). This high level of requests is mainly due to the presence of French corporate groups and the number of bank accounts held by French residents in Luxembourg.

[79] ACD data.

**Figure 7: Outgoing AEOI, 2020 - 2023[80]**




The number of outgoing AEOI averages about 3,7 million per year. Most of these reports were addressed to the fiscal authorities of Luxembourg neighboring countries, namely Germany (about 33%), France (about 14%) and Belgium (about 10%).

#### *5.1.2.2. Indirect taxes*

Overall, there are two main scenarios on how Luxembourg may be exposed to ML from indirect tax crimes committed abroad[81]:

- A non-resident person may set up a Luxembourg legal person (tax resident) to commit tax crimes in their home country (i.e. criminal use of complex and non-transparent structures). The predicate offence is thus committed by abusing a Luxembourg legal person (e.g. involvement of a Luxembourg legal person through so-called "Missing Trader Intra Community" (MTIC) or VAT carousel frauds); and
- The growth of e-commerce facilitating the cross-border sale of goods and services subject to VAT and the presence of entities in Luxembourg processing such transactions could expose the country to fraudulent businesses trying to evade their VAT obligations[82].

**Insight Box 5: MTIC fraud and Carousel fraud[83]**

MTIC fraud and carousel fraud are two forms of fraud in which a business disappears without paying the VAT due to the tax authorities or requesting a VAT refund from the government. In both cases the VAT can be seen as a profit for the "missing trader" who disappears with the money. For MTIC and carousel fraud, cross-border trade is important as intra-community trade has a zero-rate VAT taxation. There are many different and complex versions of MTIC.

**MTIC fraud**

[80] ACD data.

[81] The case of a Luxembourg legal person being misused to commit tax crimes in Luxembourg that may be laundered in Luxembourg or abroad is considered as domestic exposure.

[82] Council Directive (EU) 2020/284 of 18 February 2020 amending Directive 2006/112/EC as regards introducing certain requirements for payment service providers, link.

[83] European Parliament, *Missing Trader Intra-Community Fraud,* 2021, link.

The Commission describes a "missing trader" as a trader registered as a taxable person for VAT purposes who, potentially with a fraudulent intent, acquires or purports to acquire goods or services without payment of VAT and supplies goods and services with VAT but does not remit the VAT due to the appropriate national authority. A missing trader could potentially only exist on paper and does not necessarily be an actual functioning company. MTIC works as follows: Company A (supplier) in Member State 1 sells goods or services to Company B (missing trader) in Member State 2. As this is a cross-border transaction, the zero-rate applies to the selling of the goods or services. Company B thereafter sells the goods or services to Company C (customer) in Member State 2. Now the VAT rate of Member State 2 applies. After the sale Company B disappears without remitting the VAT due to the authorities of Member State 2.

**Carousel fraud**

In the case of carousel fraud the same goods and services are sold by a group of companies in a circle. These companies receive and claim reimbursements of VAT that have never been paid. The main difference between simple MTIC and carousel fraud is that the goods and services arrive back at the original seller and therefore concluding the circle. This circle can be very extensive with the inclusion of buffer companies. These buffer companies serve to hide the fraud from the authorities. Often the buffer company is located in the chain behind the missing trader to make the investigations of the fraud scheme more difficult. Carousel fraud could extend to more than ten companies and over multiple Member States. VAT-registered companies are allowed to claim VAT on their cross-border purchases often resulting in a request for a VAT refund. 'The purchaser not paying VAT to the supplier must declare an intra-community acquisition in the Member State of destination. This VAT is deductible.'

Carousel fraud works as follows: Company A (conduit company) in Member State 1 sells goods or services to Company B (missing trader) in Member State 2. Here the zero-rate VAT tariff applies. Company B sells the goods and services to Company C (broker company) in Member State 2 and here the VAT rate of Member State 2 applies. Company B then disappears. Company C then sells the goods or services back to Company A in Member State 1. As Company C bought the products on the domestic market of Member State 2, it had to pay VAT to Company B. The sell between Company C to Company A in Member State 1 is an intracommunity sell and therefore Company C can ask for a refund of the VAT paid to Company B. Therefore, a double loss occurs for the budget of Member State 2 as the missing trader (Company B) never remit the VAT due and the broker (Company C) requests for a refund of the VAT paid to the missing trader.

As for fraud and forgery (cf. section 5.1.1), most of the suspicious transaction/activity reports (STR/SAR) were filed by entities operating online[84] (and especially those being active in relation with e-commerce platforms) in case they note that sales occur in circumstances raising doubts about VAT compliance.

[84] Please note that throughout section 5, the definition of "entities operating online" refers to the one included in the CRF's annual reports (section 2.1.2 *prestataires en ligne*) and encompasses PIs, EMIs, VASPs, and banks operating online. The CRF's annual reports can be accessed here: link.

The AED received 1 054 requests for information from foreign counterparties (mostly neighboring countries) between 2020 and 2023, i.e. an average of 263 per year with a pic of 452 in 2021.

**Insight Box 6: Indirect taxes – risk signals identified by the AED**

**Indirect taxes: risk signals identified by the AED**

With respect to identified risk signals, the AED notes that especially with regard to trade with cars, mobile phones and luxury watches, the abuse of the margin scheme was the most commonly used mechanism, besides the MTIC fraud schemes. The abuse of the margin scheme could be detected predominantly at the import (watches/mobile phones) or after acquiring intracommunity goods under the normal VAT regime.

In the past few years, fictious trades in cross-invoicing schemes emerged. Traders are faking entire transactions including transportation and financial documentation, documents which are usually requested in presence of exempted intracommunity transactions. Third-party payments are a common pattern and despite strict AML measures, transactions paid in cash remain frequent, especially in the beverage sector.

Another trend concerns trade-based ML. In such schemes, cash from very likely illegal activities (e.g. over-/under-invoicing of goods and services, over-/under-shipment of goods and services, multiple invoicing of goods and services, etc.) is being merged with a linked trader's regular revenue on bank accounts in order to purchase goods such as FMCG (fast moving consumer goods), hygienic products or cigarettes.

The goods are sold either in genuine B2C transaction chains or through B2B grey/black market, involving cross-invoicing schemes to simulate exempted intracommunity transactions. Most of the transactions are paid in cash, very often small amounts below EUR 2 000. The newly generated cash is used for instance to pay off illicit workers in labor intensive sectors, under control of a criminal group.

**Fraud affecting the EU's financial interests – revenue fraud (VAT fraud)**

As noted earlier under section 5.1.1, the EU budget is financed from various sources such as a proportion of each EU Member State gross national income, custom duties and parts of the VAT collected by each Member State[85]. As already touched on in the Insight box above, VAT carousel fraud, or MTIC fraud, are among the most profitable crimes in the EU, costing around EUR 50 billion annually in tax losses to Member States.

Investigations relating to cross-border VAT fraud involving damages of at least EUR 10 million fall within the remit of the EPPO. In 2022, the EPPO uncovered organised crime groups with criminal activities spreading through all EPPO participating Member States as well as other European and third countries, responsible for VAT fraud estimated at EUR 6,7 billion[86].

[85] European Union, how the EU budget is financed, link.

[86] Note that EUR 2,2 billion are related to the Admiral case (see Case study below).

Actually, it is mainly in connection with the VAT fraud cases investigated by the EPPO that ML occurs, with fraudsters transferring unduly obtained funds to the bank accounts of companies set up abroad or managed by family members, or withdrawing the money in cash. In general, ML is also committed through the acquisition of real estate or luxury goods which are then resold, making it more difficult to trace the funds, or by reinvesting the profits from criminal activities in economic activities on licit and illicit markets, such as drug trafficking.

Most VAT cases investigated by the EPPO are linked to Luxembourg due to the presence of international stakeholders handling market places all around Europe[87].

The two case studies below show how Luxembourg is affected by such transnational schemes orchestrated by organised crime groups.

**Case study 2: Investigation Admiral uncovers massive VAT fraud and ML scheme, with estimated losses up to EUR 2,2 billion[88]**

In December 2023, EPPO's office in Porto (Portugal) filed an indictment against 12 suspects and 15 companies in the context of an investigation into a massive VAT fraud scheme spread through 30 countries, code-named 'Admiral'. The defendants are alleged to have used a network of companies to evade the payment of VAT while trading in electronic devices, by using fraudulent invoices and tax declarations. The fraudulent scheme took advantage of EU rules on cross-border transactions between its Member States – as these are exempt from VAT – by using a chain of traders that did not fulfil their tax obligations. The suspects are also accused of ML, by having channeled the illicit VAT profits to bank accounts in non-EU countries. According to the evidence, in order to hide the criminal origin of the profits, the defendants invested in real estate and in the sale of luxury products in the EU, amassing fortunes in the process. A private banking manager is understood to have helped the group to avoid the AML rules in place. If found guilty, the defendants face up to 25 years imprisonment. The estimated damage in Portugal alone amounts to over EUR 80 million. The estimated losses to the EU and to the national budgets under the Admiral investigation amounts to EUR 2,2 billion.

In this case, a set of Luxembourg companies were used as conduit companies, but also actively intervened in the ML scheme with at least 11 bank accounts identified. For the trade, the fraudsters extensively used the service of PIs based in Luxembourg, with at least 41 accounts identified, in which more than EUR 500 million circulated. That amount was the product of the sales and constituted, ultimately, the origin of the crime proceeds. It was furthermore highlighted during the investigation that the criminal organization behind the fraudulent scheme managed to incorporate two Luxembourg companies, via Luxembourg 'company providers', for the purposes of bringing the illicit gains from a third country to Luxembourg by reinvesting them in real estate and other financial products.

The investigation of this case is still ongoing and the suspects are entitled to the presumption of innocence.

[87] Press release 29/11/2022 of the European Public Prosecutor's Office, Operation Admiral, link.
[88] EPPO.

**Case study 3: Investigation Admiral 2.0: Europe's biggest VAT fraud with links to organised crime**[89]

Taking advantage of its decentralised model and central analytical capacity, the EPPO was able to establish links between persons and companies under investigation Admiral, and a criminal syndicate based in the Baltics. The investigation revealed that this syndicate used the same modus operandi, and partly also the same organisation and infrastructure, as the perpetrators investigated under Admiral, to carry out a massive VAT carousel fraud – a complex criminal scheme that takes advantage of EU rules on cross-border transactions between its Member States, as these are exempt from VAT.

According to the investigation, the suspects established companies in 15 EU Member States, acting as legitimate suppliers of electronic goods. They sold over EUR 1,48 billion worth of popular electronic devices via online marketplaces to customers located in the EU. While the end customers paid VAT on their purchases, the selling companies would not fulfil their tax obligations. By simply disappearing, they would avoid transferring the amounts due to the responsible national tax authorities. Other companies in the fraudulent chain would subsequently claim VAT reimbursement from the national tax authorities, creating an estimated VAT damage of EUR 297 million. In this case, the proceeds of the crime were partly deposited on a number of accounts held by PIs located in Luxembourg for a total amount of EUR 600 million, which were, from there, laundered through different third countries. The EPPO suspects over 400 companies to be part of this complex fraudulent scheme, which is also believed to have been used for laundering proceeds stemming from drug trafficking, different types of cybercrime, and investment fraud.

All persons concerned are presumed innocent until proven guilty in the competent courts of law.

According to EPPO's annual report 2023, by 31 December 2023, the EPPO had a total of 1 927 active investigations for an overall estimated damage of EUR 19,2 billion. The EPPO notes in its 2023 annual report that as of 31 December 2023, 339 (i.e. 18%) active investigations related to VAT fraud with a total estimated damage of EUR 11,5 billion. With regard to Luxembourg more precisely, the EPPO notes that among the 13 active investigations, two related to VAT fraud with a total estimated damage of EUR 30 million[90].

The EPPO further indicates in its 2023 annual report that this type of fraud was predominantly committed through the use or presentation of false, incorrect or incomplete VAT documents. This type of crime was also committed by sophisticated criminal organisations acting across borders. The EPPO identified, amongst others, the automotive sector, dealers selling electronic and textile merchandise, and pharmaceutical products, IT hardware and software, as well as dealers selling alcoholic and non-alcoholic beverages as sectors most exposed to this type of fraud.

[89] Investigation Admiral 2.0: Europe's biggest VAT fraud with links to organised crime | European Public Prosecutor's Office, link.

[90] EPPO, *2023 Annual Report*, link.

Last but not least, the EPPO and the AED mentioned cases where Luxembourg legal persons were involved in a VAT carrousel, and served as conduits, with the origin and the final destination of the funds being in a foreign country.

#### *5.1.2.3. Luxembourg's external threat exposure to tax crime*

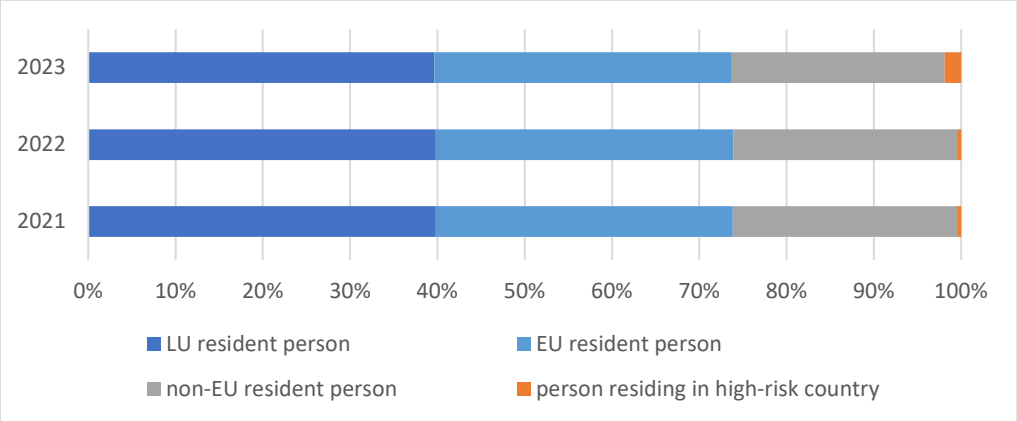
Luxembourg legal persons may be abused to commit crimes in relation with direct and indirect tax crimes. Data from the LBR suggests that the number of legal persons registered with the Trade and Companies Register ("*Registre de Commerce et des Sociétés*", RCS) has increased throughout the observation period. Considering Luxembourg's openness to international business and risks related to tax crimes with regard to non-resident persons, the graph below outlines the share of Luxembourg legal persons with a beneficial owner (BO), respectively senior management official (SMO) ("*dirigeant principal*") residing in Luxembourg, the EU, or outside of the EU.

**Table 9: number of legal persons registered with the RCS as at 31/12, 2020-2023**

| Year | Number of legal persons registered with the RCS | Variation (compared to prior year) |
|---|---|---|
| **2021** | 139 430 | +0,2% |
| **2022** | 144 438 | +3,6% |
| **2023** | 146 297 | +1,3% |

The figures below provide a breakdown of the country of residence of Luxembourg legal persons BO[91] and SMOs[92] as registered with the LBR. Most of these entities are controlled, owned or managed by either a Luxembourg or EU resident.

**Figure 8: Share of legal persons where BOs reside in Luxembourg, EU, non-EU and high-risk countries, 2021-2023[93]**

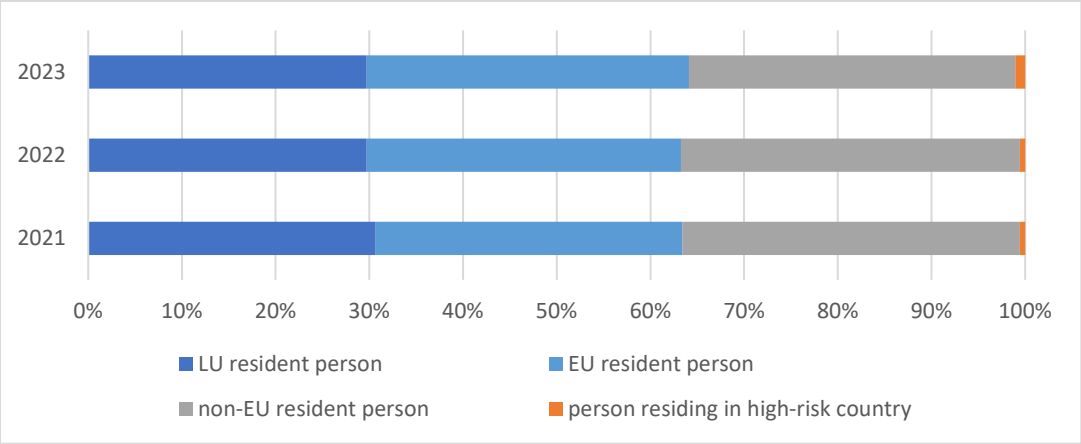



[91] Pursuant to article 1, paragraph 7, letter a), point i) of the 2004 AML/CFT Law.

[92] Pursuant to article 1, paragraph 7, letter a), point ii) of the 2004 AML/CFT Law.

[93] Please note that a legal person is assumed to be owned or controlled by a person from a high risk-country if at least one person resides in a high-risk country. A high-risk country is a country that was listed by FATF as jurisdiction under increased monitoring.

**Figure 9: Share of legal persons where SMOs reside in Luxembourg, EU, non-EU and high-risk countries, 2021-2023[94]**




Between 2020 and 2023, the CRF received almost 20 000 reports in relation with tax crimes. Although the number of reports has more than doubled, from around 2 300 reports in 2020 to almost 5 700 in 2023, the CRF considers that the increase is the result of increased awareness and sensibilisation efforts among obliged entities. Supervisors, professional organisations and the CRF are indeed continuously organising and participating in trainings and conferences with the private sector in order to raise awareness on the latest typologies and trends with regard to tax crimes. For instance, on 3 July 2020 the CSSF issued circular 20/744 to complement circular 17/650 with additional indicators of laundering of an aggravated tax fraud or tax evasion[95]. In addition, the increase could also be explained by the increasing vigilance of e-commerce platforms and their enhanced cooperation with tax authorities following the introduction of new rules regarding their responsibility for the correct application and remittance of VAT by foreign traders (e.g. EU Directive 2020/284).

Prosecution authorities received 118 MLA requests in 2020 – 2023 related to tax crimes. In 2020 and 2021, prosecution authorities seized assets worth EUR 5,49 million (6 seizures) as a result of MLA requests related to tax crimes, compared to EUR 3,26 million (11 seizures) in 2018 and 2019[96].

The overall external threat level is assessed to be "Very High".

or as a high-risk jurisdiction subject to a call for action as at year end of the analysed year. A legal person is assumed to be owned or controlled by a resident from a non-EU country if at least one person resides in a non-EU country. A legal person is assumed to be owned or controlled by a EU resident if at least one person is from an EU country, but none from a non-EU country and none from a high-risk country. A legal person is assumed to be owned or controlled by a resident person if all persons owning or controlling the legal person are Luxembourg residents.

[94] Please note that a legal person is assumed to be managed by a SMO from a high risk-country if at least one SMO resides in a high-risk country. A high-risk country is a country that was listed by FATF as jurisdiction under increased monitoring or as a high-risk jurisdiction subject to a call for action as at year end of the analysed year. A legal person is assumed to be managed by a SMO official from a non-EU country if at least one SMO resides in a non-EU country. A legal person is assumed to be controlled by EU SMOs if at least one SMO is from an EU country, but none from a non-EU country and none from a high-risk country. A legal person is assumed to be managed by Luxembourg resident SMOs if all SMOs are Luxembourg residents.

[95] Circular CSSF 20/744, link.

[96] *Parquet Général* Statistical Service.

### *5.1.3. Corruption and bribery*

| This section should be read in conjunction with sections 5.1.1 and 5.1.5. |
|---|

Corruption is estimated to cost the EU between EUR 179 billion and EUR 990 billion per year, amounting to up to 6% of its GDP[97]. Corruption is considered as one of the most significant enablers of organised crime in all regions of the world[98].

Europol considers that corruption is an integral element of almost every organised criminal activity taking place at all levels of society. It can range from petty bribery to complex multi-million-euro corruption schemes. Many criminals use corruption only occasionally, but a smaller proportion of criminal networks engage in frequent and proactive corruption targeting public servants or specific sectors as an intrinsic part of their business strategy. Overall Europol assessed that almost 60% of criminal networks engage in corruption[99]. Similarly, the European Commission highlights the rising use of corruption by high-risk long lasting criminal networks[100]. The Serious Organised Crime Threat Assessment (SOCTA) emphasizes the use of crypto assets to make payments to corrupt officials and for ML-purposes[101].

In 2023, the EPPO counts 131 active investigations into corruption related offences that damage, or are likely to damage, the EU's financial interests. These relate to cases where the public officials are suspected of having acted illegally in favour of private beneficiaries, or in situations of a conflict of interest, and where the offence of abuse of official authority or power is registered. Bribery was also investigated by the EPPO, as an instrumental offence in awarding contracts and projects to specific subjects, both in procurement and in non-procurement fraud[102]. According to EPPO's annual report 2023, EPPO was investigating one corruption case with known implications to Luxembourg.

In Luxembourg, the external threat exposure stemming from corruption and bribery may be impacted by several factors:

- Affluent and wealthy bribers or bribed individuals could invest/place proceeds generated from corruption and bribery in Luxembourg or use the generated returns for this type of illicit activities. Considering this, sophisticated sectors collecting and investing funds for wealth and asset management purposes may be targeted by those persons.
- Legal and financial professionals (from Luxembourg or abroad) could provide advice, set up legal persons or facilitate the takeover of legitimate companies in Luxembourg for the purpose of laundering the proceeds of corruption.
- Luxembourg legal persons could be used as companies for ML of proceeds of corruption in a wider scheme, i.e. complicit (or abused) legal and financial professionals setting up the structure of holding companies.

[97] European Commission, Corruption, link retrieved on 3 May 2024.
[98] Interpol, *2022 INTERPOL GLOBAL CRIME TREND SUMMARY REPORT*, link.
[99] Europol, Crime areas – corruption, link retrieved on 23 September 2024.
[100] European Commission, Corruption in organised crime, link retrieved on 23 September 2024.
[101] Europol, *Serious Organised Crime Threat Assessment 2021*, link.
[102] EPPO, *Annual Report 2023*, link.

- Considering the limited size of the domestic market, Luxembourg is an internationally oriented economy. Luxembourg businesses could, therefore, be misused to (wittingly or unwittingly) launder proceeds generated from corrupt activities, corruption-related proceeds or act themselves as bribers or bribed persons.

#### *5.1.3.1. Luxembourg's external threat exposure to corruption and bribery*

The number of reports filed with the CRF throughout the observation period regarding corruption and bribery is rather low (around 900 reports during the observation period) in comparison to the total number of reports filed[103]. Although entities operating online[104] are, in general, those filing most reports with the CRF, the number of filings made by these entities with regard to corruption and bribery is quite limited (86 out of 166 786 reports filed by these entities). It appears that the prevalence of reports related to corruption is higher in the more sophisticated sectors, such as Alternative Investment Fund Managers (AIFMs) and PFS, with 10% and 7% of reports filed by the respective sub-sector being related to corruption. The CRF also observed that the number of reports filed by DNFBPs and AIFMs is increasing.

**Insight Box 7: Corruption related STR/SARs - red flags and modus operandi identified by the CRF (non-exhaustive list)[105]**

Typically involved red flags are for instance:

- Open source data;
- The presence of PEPs, or persons related to sectors typically targeted by corruption such as transport, telecommunication, public administration, or the natural resources (i.e. oil and gas); or
- The use of offshore corporate nominee accounts ultimately held by foreign PEPs or individuals associated with corruption allegations, for investment purposes via legal persons and legal arrangements.

Identified modus operandi:

- The abuse of legal persons and legal arrangements, i.e., the use of opaque arrangements through complex structuring with multiple legal persons in different jurisdictions;
- The use of shell companies, with or without the use of nominees, aiming at concealing the BO and notably diluting links with potentially illicit activities;
- The use of consultancy, loan, and shareholder contracts often without economic activity. Reviewing supporting documents can reveal inconsistencies that constitute new indicators of ML.

[103] Please note that obliged entities are not required to qualify the predicate offence. The suspected underlying predicate offence is identified based on the assessment of relevant elements during the case analysis and may be subject to revision as additional information becomes available throughout the course of the analysis. In addition, corruption and bribery offences are largely interconnected with other predicate offences and therefore detection might be challenging.

[104] Please note that throughout section 5, the definition of "entities operating online" refers to the one included in the CRF's annual reports (section 2.1.2 *prestataires en ligne*) and encompasses PIs, EMIs, VASPs, and banks operating online. The CRF's annual reports can be accessed here: link.

[105] CRF data. It should be noted, that these red flags and modus operandi are often observed in cases with an international exposure (i.e. international financial flows are transiting through Luxembourg "in/out transfers"); use of frontmen/front companies; fictious consultancy agreements; fictous loan agreements; etc).

- The use of intermediaries, professionals who are experts in legal and financial matters, intervening and assisting their clients at different stages of the business life cycle.

The following is an illustrative case study provided by the CRF.

**Case study 4: External threat – corruption and bribery**

The CRF initiated an international cooperation case regarding suspicions related to three insurance policies valued at over EUR 100 million subscribed several years ago and held by a Luxembourg-based fiduciary. The BO of these policies was a PEP from country A. Additionally, information was gathered that the policyholder would change from the fiduciary to the BO before the total surrender of the policies. Furthermore, adverse media was identified indicating that the BO was under investigation in country A for allegations of influence peddling, false statements, attempted fraud involving public funds and corruption. The information collected was immediately exchanged with the concerned FIU for further analysis.

Throughout the observation period, the CRF froze significant amounts with respect to corruption and bribery between 2020 and 2023: EUR 31,8 million in 2020 (13 freezes) and EUR 9,66 million (4 freezes) in 2021, EUR 106,58 million in 2022 (4 freezes) and EUR 502,79 million (10 freezes) in 2023[106]. In this context, it is also interesting to mention that 65% of freezing orders between 2020 and 2023 were initiated by the CRF. The remaining 35% were based on international requests from foreign financial intelligence units (FIUs). Out of these 35%, more than half of them were requested by a foreign FIU after the CRF had previously sent a spontaneous information exchange to the relevant foreign FIU. Overall, 100% of frozen amounts between 2020 and 2023 regarding corruption related to international cases, i.e. money stemming from corruption that took place in other jurisdictions.

**Insight Box 8: CSSF thematic review focused on PEPs and the fight against corruption**

The CSSF's "UCI On-site Inspection" department carried out in March and April 2022 a thematic review focused on PEPs and the fight against corruption, the focus area of which was Investment Fund managers' (IFM) adherence with PEP related legal and regulatory framework. Despite minor elements (e.g. lack formalization at the level of the company materializing specifically the senior management approval of PEPs), the main takeaway of the review was that the overall understanding of the risks associated with PEPs as well as the related mitigation measures put in place by the entities inspected were satisfactory. Due to the solid legal and regulatory framework with regards to PEPs, the awareness on that topic of professionals under CSSF supervision appears to be good. Where deficiencies in the measures taken by professionals in that regard are detected by the CSSF, this can lead to administrative sanctions. The awareness on the risk of laundering the proceeds of active corruption should be further developed, e.g. geographical risk, risk linked to certain industry sectors.

[106] CRF, *Annual Report*, 2019, link, 2020, link, 2021 and 2022, link, 2023, link.

The number of MLA requests and seizures related to corruption and bribery have decreased since the 2020 NRA update. Between 2020 and 2023, prosecution authorities received 47 MLA requests related to corruption and bribery (of which 27 ML-related). The overall external threat level is assessed to be "Very High".

### *5.1.4. Drug trafficking*

| Please note that this section should be read in conjunction with sections 5.1.1 and 5.1.5. |
|---|

The European Council reports an estimated yearly retail value of at least EUR 30 billion as well as ever larger seizures. It also notes that European markets are characterized by a high availability of various types of drugs, the increasing use of violence and technology[107].

According to Europol, nearly half of the reported most threatening criminal networks in the EU are involved in drug trafficking trade. The trade in cocaine, cannabis, synthetic drugs and new psychoactive substances are key threats to the EU due to the levels of drug-related violence (i.e. mainly used as retaliation for lost or un-finalised shipments, but also to gain dominance over a territory or the supply chain), the multibillion-euro profits generated and the substantial harm caused by it[108,109].

In Luxembourg, the external threat exposure stemming from drug trafficking (and ML of related proceeds) may occur through its financial centre or by cash. On the one hand, the international character of its financial centre exposes the Grand-Duchy to a considerable number of incoming and outgoing financial flows. Proceeds generated from drug trafficking could transit through Luxembourg's financial centre by abusing services offered by Luxembourg professionals. On the other hand, national ML/TF Risk Assessments from Luxembourg's neighbouring countries consider the threat related to drug trafficking as significant. These reports further indicate that proceeds stemming from drug trafficking are laundered with cash. Considering the proximity of sizable drug markets near Luxembourg, cash proceeds stemming from this type of predicate offence could be laundered in or transit through Luxembourg.

**Case study 5: Members of drug trafficking network arrested for ML in Germany and Luxembourg[110]**

At the request of France, authorities in Germany and Luxembourg carried out a coordinated blow on a criminal network, which was set up to launder proceeds from drug trafficking.

At the request of Lille's Interregional Specialised Prosecution Service in France, LEAs in Germany and Luxembourg arrested four members of a criminal group suspected of laundering the proceeds from drug trafficking. The crime group consisted of its leader, nicknamed "the Minister", as well as intermediaries and lorry drivers who were facilitating the trafficking of drugs and cash through various European countries.

[107] The European Council, the EU's fight against organised crime, link retrieved April 2024.
[108] Europol, *Serious and organised crime threat assessment (EU SOCTA),* 2021, link.
[109] Europol, *Decoding the EU's most threatening criminal networks,* 2024, link.
[110] Europol, Follow the money: members of drug trafficking network arrested for money laundering in Germany and Luxembourg, link.

The investigation began in France in 2017 after customs agents found GBP 225 990 inside a lorry owned by a company registered in Luxembourg. A cocaine seizure made in France in 2019, and the ensuing information exchange, pointed authorities to the possible links between the two seizures. The financial investigations were supported by Europol's European Financial and Economic Crime Centre. This allowed the authorities to draw clear links between drug trafficking and the ML activities of the group.

The operational action took place on 23 March 2021 and resulted in:

- 14 searches carried out in Germany and Luxembourg;
- 4 members of the crime group, including its leader, arrested on the basis of European arrest warrants issued by France;
- 4 properties worth several million of euros and high-value vehicles seized;
- Several bank accounts frozen with a total value of EUR 187 000;
- EUR 26 000 cash seized; and
- 50 mobile phones and other devices seized for further examination.

#### *5.1.4.1. Luxembourg's external threat exposure to drug trafficking*

During the observation period, the AML section of the judicial police service (SPJ) conducted inter alia three parallel investigations on major cases of illicit drug trafficking where foreign proceeds were laundered through the abuse of the Luxembourg financial centre. In all of these cases, the involvement of legal persons or corporate structures was identified. Other encountered typologies were the use of forged documents (such as employments contracts, invoices, notarial deeds) to give a legal appearance to the transactions or to hide the illicit origin of large cash deposits that were likely to be linked to drug trafficking.

As outlined in section 3, the FATF mutual evaluation reports of Luxembourg's key inward investment countries cite drug related offences as a key ML threat. The extent and significance of these financial flows with these countries could contribute to the exposure linked to ML of proceed from drug trafficking committed abroad.

Considering the prevalent role of cash in the laundering of proceeds generated from drug trafficking, the number of reports filed with the CRF is rather low (about 3 600 reports) in comparison to the total number of reports filed. Judicial authorities received 106 MLA requests during the observation period. The Grand-Ducal Police cites drug trafficking as top-five crime area with regard to incoming and outcoming requests through the Europol's secure information exchange network.

In line with the global situation and the Luxembourg specific context, the external threat level for drug trafficking remains "High".

### *5.1.5. Participation in organised criminal group and racketeering*

Please note that this section should be read in conjunction with sections 5.1.1, 5.1.3, 5.1.4, and 5.2.1.

According to Europol, along with terrorism, serious and organised crime continues to constitute the most pressing internal security challenge to the EU. Crime groups often operate across borders. It is estimated that about 70% of criminal groups are, in fact, active in more than three EU Member States[111]. The European Council recognises organised crime as a major threat to European citizens, business and institutions, as well as to the European economy. In 2019, criminal revenues in the main criminal markets amounted to 1% of the EU's GDP, i.e. EUR 139 billion[112].

Overall, it should be noted that this predicate offence is particularly interconnected with other types of predicate offences as the aim of being member in an organised criminal group is generally to engage in criminal activities.

#### *5.1.5.1. Luxembourg's external threat exposure*

Although the number of reports filed with the CRF with regard to participation in an organised criminal groups is very low (less than 180 reports filed between 2020 and 2023), the CRF disseminated a relatively high share of cases to foreign counterparts. Overall, it should be borne in mind that the CRF is at the very beginning of the investigative chain. It receives reports based on suspicious transactions or activities. The link to an organised criminal group is often identified at a later stage of the analysis. This is also confirmed by the SPJ.

Between 2020 and 2023, judicial authorities received 167 MLA requests related to this crime (of which 94 ML-related), compared to 95 (of which 56 ML-related) in 2018 and 2019[113].

In line with the global situation and the Luxembourg specific context, the external threat level for participation in organised criminal groups remains "High".

### *5.1.6. Counterfeiting and piracy of products*

With regard to counterfeit goods, Europol notes that seizures of intellectual-property rights materials have continuously increased in recent years, both at the EU's external border and in the internal market, along with seizures of labels, tags and stickers. In addition, the digitalization of trade and transport has shifted most of the distribution of counterfeit goods online, further distancing criminals from their commodities. The distribution of counterfeit goods mainly occurs on the surface web and Europol notes that China (including Hong Kong, and Vietnam to a lesser extent) have remained the main countries of origin in recent years[114].

The growing demand for online entertainment during the COVID-19 pandemic led to an increase in distribution of illegal IPTV. However, improved access to legal platforms and enforcement scrutiny in some EU Member States, led to a drop in users for these illicit platforms. The websites illegally distributing video

[111] Europol, *Serious and organised crime threat assessment (EU SOCTA)*, 2021, link.
[112] European Council, The EU's fight against organised crime, link retrieved on 15 December 2022.
[113] *Parquet Général* Statistical Service.
[114] Europol, *The Other Side of the Coin,* 2024, link.

content are hosted on servers across Europe, Asia and the Middle East. Much of the criminal profit is generated by online advertising, paid subscriptions, and malware attacks[115].

It should also be noted that e-commerce has grown substantially in the past few years, especially for low-value shipments (less than EUR 150) from non-EU countries and imported into the EU. While 9% of European residents placed orders online outside the EU in 2002, this figure rose to 70% in by 2021. The number of low-value imported shipments has risen from 150 million in 2015 to 2 billion in 2022[116].

In Luxembourg, the external threat stemming from counterfeiting and piracy of products is impacted by the presence of FIs (including MVTS) processing transactions related to marketplaces where goods and services subject to trademarks and intellectual property are sold.

#### *5.1.6.1. Luxembourg's external threat exposure*

The number of reports filed with the CRF related to counterfeiting and piracy of products accounts for around 20% of total declarations received between 2020 and 2023. In fact, it is the second most encountered predicate offence by the CRF after fraud and forgery. As outlined in section 6.1.3.1, Luxembourg's MVTS sector serves a considerable number of clients. Together with the sophisticated transaction monitoring tools in place, this sector files a considerable number of reports with the CRF, with most of them having no direct link to Luxembourg (except for the Luxembourg headquarter of the entity and the Luxembourg account). The CRF performed 48 freezes amounting to nearly EUR 3 million.

**Case study 6: External threat – counterfeiting and piracy of products[117]**

Triggered by an international FIU-to-FIU cooperation, the CRF analysed a case involving suspected counterfeit products, specifically plagiarized IT accessories, in which a turnover exceeding EUR 195 000 was generated within 7 months. The CRF collected all available data and information and disseminated the relevant intelligence to the concerned FIU, which then coordinated with their competent Public Prosecutor's Office. Based on the disseminated findings, a freeze order was requested to the CRF in order to secure the remaining balance of approximatively EUR 130 000, while the concerned jurisdiction issued an MLA request to seize the funds.

The number of foreign requests on counterfeiting and piracy of products received by Luxembourg prosecution authorities is relatively low, with a total of 5 requests (among which 2 were ML related) between 2020 and 2023.

In line with the global situation and the Luxembourg specific context and considering the above, the threat level for counterfeiting and piracy of products remains "High".

[115] Europol, *The Other Side of the Coin,* 2024, link.
[116] MoF, *Annexe – Rapport d'activité 2023,* 2024, link.
[117] Case study provided by the CRF.

### *5.1.7. Sexual exploitation, including sexual exploitation of children*

The following section analyses two different types of sexual exploitation namely sexual exploitation of adults and sexual exploitation of children.

International organisations such as Europol and Luxembourg authorities noted the increasing role played by social media and streaming platforms such as Snapchat, Telegram, OnlyFans, Youtube and Minecraft. With regard to this predicate offence, these platforms are used:

- to initiate the first contact with the victim (observed typologies: Loverboy method, grooming);
- to market services and/or generated content to potential buyers or interested parties; and
- to distribute sexual abuse material such as videos, livestream or pictures.

Luxembourg's financial centre is exposed to the external threat stemming from sexual exploitation, including sexual exploitation of children as:

- proceeds generated from sexual exploitation could transit through Luxembourg's financial centre (e.g. accounts from buyers or sellers located in Luxembourg);
- Luxembourg-based entities could process transactions linked to the sale and distribution of sexual abuse material;
- Luxembourg legal persons (e.g. holding vehicles) could receive revenues or funds linked to the sale and distribution of sexual abuse material.

#### *5.1.7.1. Sexual exploitation of adults*

Sexual exploitation of adults is a form of human trafficking and generally occurs when a person induces another person:

- to engage in prostitution or continue to do so; or
- to perform sexual acts through which they are exploited, in the presence or in front of the perpetrator or a third person, or to have such acts performed on themselves by the perpetrator or a third person.

This offence therefore requires at least two individuals, a victim and a person who exploits the victim's economic or personal situation. Depending on the social and economic situation of the victim, these criminals may approach their victims differently. Overall, there are two different methods on how victims (especially young girls) are forced into prostitution:

- through the Loverboy method: the latter involves creating a fake romantic relationship to emotionally manipulate the victim into prostitution; and
- considering the economic crisis in their home countries and/or through false promises: victims are lured away from home with promises of a better life abroad (e.g. careers as models or jobs in the hospitality industry). Upon arrival in the destination country, victims are forced to work into

brothels, apartments or on the streets. Often, they do no longer have documents and are, thus, illegal in the country[118].

#### *5.1.7.2. Sexual exploitation of children*

Europol notes that live-distant child abuse remains a persistent threat[119]. Since 2020 and following the Covid-19 Pandemic, the CRF has indeed observed a steady increase in child sexual abuse material (CSAM) livestreaming. The sellers, who livestream the CSAM, are located in ML high-risk jurisdictions, while their customers (who buy specific content and who communicate with the sellers via chat) are located within the EU. In some cases, the CSAM buyers themselves distribute the purchased CSAM content via specific websites or through social media.

In 2021, 85 million pictures and videos depicting child sexual abuse were reported worldwide. Moreover, reported child sexual abuse cases increased by 64% from 2020 to 2021[120]. According to Europol[121], CSAM has increased substantially. It is often self-generated by means of manipulation or blackmail and LEA reported a peak of online grooming cases in 2020, especially via social media and gaming platforms. Between 2020 and 2021, the number of self-reported recordings increased by 168%, according to the Internet Watch Foundation. In 2022, the number of self-reported recording continued to increase, although to a lower extent (increase of 6% in 2022 and 8% increase in 2023)[122]. The monetisation of CSAM is a growing threat: it is estimated that the annual revenue of CSAM sites have more than tripled between 2017 and 2020[123].

Artificial intelligence (AI) models able to generate or alter images were also abused by offenders to create CSAM[124]. In this regard, the CRF noticed a rise in the sale and distribution of AI-Generated CSAM, depicting both fictional and life-like minors. Moreover, the CRF further noticed a trend that CSAM distributors and sellers use major video streaming and social media platforms to promote CSAM content by sharing non-explicit but suggestive videos of minors often portrayed in a family setting.

**Insight Box 9: Red flag indicators – Characteristics and activity indicators for live streaming of child sexual abuse and exploitation (CSAE)[125]**

These red flag indicators are based on a strategic analysis of several similar cases by the CRF in the past few years:

- personal cross-border payments;
- mostly repeated and in even amounts, usually less than EUR 70 predominantly from many

[118] Mission Freedom, Forced prostitution, link retrieved on 5 August 2024.
[119] Europol, *Internet organised crime threat assessment (IOCTA) 2024*, 2024, link.
[120] European Council, The EU's fight against organised crime, link retrieved December 2022.
[121] Europol, *Internet organised crime threat assessment (IOCTA) 2021*, 2022, link.
[122] Internet Watch Foundation, *self-generated sexual abuse online – annual report 2021, link* and Internet Watch Foundation, *self-generated sexual abuse online – annual report 2022,* link and Internet Watch Foundation, *self-generated sexual abuse online – annual report 2023,* link.
[123] Europol, *Internet organised crime threat assessment (IOCTA) 2021*, 2022, link.
[124] Europol, *Internet organised crime threat assessment (IOCTA) 2024*, 2024, link.
[125] CRF.

different male senders based in Western countries;

- to receiving EMI accounts registered in a high risk CSAE jurisdiction without any plausible business purpose or commercial explanation;
- notes relating to children and/or to other help/family help;
- suspects' email addresses and on-line monikers identified matching profiles on dating and adult platforms, including for instance broadcasting service platforms where users stream own live video content or interact with the video streams of other users in real time or platforms to meet people who are traveling or speak other languages, which can often be used by buyers to pursue CSAM content or meet CSAM facilitators, such as for instance: dating sites, gaming sites etc.

#### *5.1.7.3. Luxembourg's external threat exposure*

Obliged entities filed over 2 100 reports with the CRF, with entities operating online[126] accounting for over 99% of them. Generally, the CRF observed that transactions linked with escort services, transport services, hospitality services, and online renting were reported by obliged entities with respect to sexual exploitation of adults. In the case of sexual exploitation of children, the CRF observed transactions masked as "family support" and payments linked to "premium services or premium servers" on filesharing platforms, social media and streaming platforms. For over 90% of the reports filed with the CRF, the only link with Grand-Duchy is the Luxembourg PI processing the transaction. The CRF actively disseminates relevant information to their foreign counterparts or Europol, especially in cases where the implication of organised crime groups is suspected.

Between 2020 and 2023, prosecution authorities received 33 MLA requests related to sexual exploitation (one was ML-related), compared to 80 (of which four ML-related) in 2018 and 2019.

Considering the above, the external threat level for sexual exploitation, including sexual exploitation of children, remains "High".

### *5.1.8. Cybercrime*

Please note that this section should be read in conjunction with sections 5.1.1, 5.1.7, and 5.2.1.

This section analyses the external threat stemming from attacks against information systems, such as a distributed denial-of-service (DDoS) attack, hacking attacks, and criminals providing malware and ransomware software as a service to interested parties. It should be born in mind that attacks against information system is often a mean to commit other predicate offences such as extorsion or fraud. Fraud that is enabled through or conducted in the cyber environment (i.e. CEF) is analysed in section 5.1.1 above.

[126] Please note that throughout section 5, the definition of "entities operating online" refers to the one included in the CRF's annual reports (section 2.1.2 *prestataires en ligne*) and encompasses PIs, EMIs, VASPs, and banks operating online. The CRF's annual reports can be accessed here: link.

**Insight Box 10: Crime-as-a-service**[127]

Cybercrime services are widely available and have a well-established online presence (especially on the dark net), with a high level of specialisation inside criminal networks and collaboration between illicit providers. The services offered to perpetrate cybercrime are often intertwined and their efficacy is to a degree co-dependant. The illicit service providers cater to a large number of criminal actors by offering services, such as:

- Malware-as-a-service;
- Phishing-as-a-service; or
- Ransomware-as-a-service.

Crime as-a-service providers are aware of the needs of criminals and actively advertise their services on criminal markets.

Europol estimates that cybercrime is likely to be under-reported and that it represents an increasing threat for individuals, businesses, and governments. Related crimes have become more and more sophisticated[128]. The criminal landscape remains wide-ranging, comprising both lone actors and networks with various levels of expertise and capability. Some cybercriminals targeting the EU are EU-based, while others operate from abroad, concealing their illicit operations and funds in third countries[129].

In a similar vein, the European Council[130] confirms that cybercrime is set to grow further in the future, given that 22,3 billion devices worldwide are expected to be linked to the Internet of Things by 2024. The carry-over effects of the geopolitical situation could be seen by the barrage of disruptive cyberattacks against not only Ukrainian and Russian targets, but also worldwide, especially in the EU. The boost in these malicious activities targeting EU Member States is mostly due to a significant number of DDoS attacks affecting national and regional public institutions. As for CEF (see section 5.1.1), the use of crypto assets is prevalent[131].

#### *5.1.8.1. Luxembourg's external threat exposure*

Considering the above, Luxembourg financial centre may be exposed to the external threat stemming from cybercrime via the following scenarios:

- Victims of cybercrime: funds held with Luxembourg bank or payment accounts may be transferred to crypto assets exchange platforms to pay the ransom; and
- Criminals: considering the range of services offered by Luxembourg's financial centre, criminals may place/invest generated funds in Luxembourg or channel them to other financial centres.

[127] Europol, *Internet organised crime threat assessment (IOCTA) 2024*, 2024, link and Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023*, 2023, link.
[128] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023*, 2023, link.
[129] Europol, *Internet organised crime threat assessment (IOCTA) 2024*, 2024, link.
[130] The European Council, the EU's fight against organised crime, link retrieved on 15 December 2022.
[131] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023*, 2023, link.

Between 2020 and 2023, entities operating online[132] and banks filed over 99% of the around 1 400 reports with the CRF. STRs are usually triggered in cases in which victims transfer funds held with their Luxembourg bank or payment account to crypto assets exchange platforms to pay the ransom. Nonetheless, the CRF observed that there has been a clear shift of criminals using decentralized and not regulated exchanges in order to launder the proceedings of ransomware or offences in relation to cybercrime, such as hacking and DDoS attacks. The perpetrators of these offences are thus not using the services of regulated exchanges but decentralized applications. The latter offer the benefit that the suspects do not need to provide any KYC information and supporting evidence and the funds can be easily swapped between different crypto assets. Nonetheless, this adds further complexity in terms of detection.

The external threat level for cybercrime, remains "High".

### *5.1.9. Analysis of other external offences: medium threat exposure*

The following section resumes the external threat assessment for predicate offences where the overall external threat level was assessed to be "Medium".

#### *5.1.9.1. Smuggling*

According to Europol, 80% of reported criminal networks are involved in, amongst others, excise fraud[133].

Goods such as alcohol, cigarettes and fuel are subject to excise duty upon production in, or on import to, the EU. Large scale excise fraud (with a focus on the production and/or trafficking of illicit tobacco products in the EU is among one of the European Multidisciplinary Platforms Against Criminal Threats (EMPACT). Europol notes that the main areas of excise fraud in Europe include[134]:

- the smuggling or illegal importation of excise goods;
- the illegal manufacture of excise goods; and
- diversion, which involves diverting goods without paying excise duty.

Price differences between Member States and between Member States and neighboring non-EU countries are the main drivers for criminals involved in this type of crime. For example, figures from Eurostat show that price levels for alcoholic beverages and tobacco vary among EU Member States and are more significant for tobacco than for alcoholic beverages[135].

The number of reports received by the CRF in relation with this type of predicate offence is relatively low, with a total of 7 reports filed between 2020 and 2023. There were no related freezes. Throughout the observation period, judicial authorities received 3 MLA requests regarding this predicate offence. There were no related seizures.

[132] Please note that throughout section 5, the definition of "entities operating online" refers to the one included in the CRF's annual reports (section 2.1.2 *prestataires en ligne*) and encompasses PIs, EMIs, VASPs, and banks operating online. The CRF's annual reports can be accessed here: link.

[133] Europol, *Serious and organised crime threat assessment (EU SOCTA)*, 2021, link.

[134] Europol, Excise fraud, link retrieved July 2024.

[135] Eurostat, Comparative price levels for food, beverages and tobacco, link retrieved June 2024.

Considering the size and the number of flows transiting through Luxembourg's financial centre, proceeds generated from excise fraud could transit through the latter.

#### *5.1.9.2. Insider trading and market manipulation*

Luxembourg's exposition stems from the presence of the financial centre, but trading activity on domestic markets (i.e. markets operated by the Luxembourg Stock Exchange) is limited. The CRF received over 270 reports with more than half of them being filed by banks followed by the investment sector.

More than 250 suspicious order and transaction reports (STORs) related to potential market abuse cases were filed by Luxembourg based professionals from 2022 and to 2023 with the CSSF. The vast majority of these reports concerned transactions executed on markets operated in other Member States and were transmitted to the relevant competent authorities. Furthermore, the CSSF assisted other authorities in 86 requests for cooperation in potential market abuse cases in from 2020 to 2023, which further illustrates the international dimension of market abuse cases and the CSSF's extensive international cooperation in this context.

#### *5.1.9.3. Robbery and theft and illicit trafficking of stolen goods*

In the context of the external threat assessment, the predicate offence is committed abroad and the laundering of the generated proceeds would take place in Luxembourg.

Luxembourg is exposed to the external threat of "theft and robbery" and "illicit trafficking in stolen and other goods" through the presence of entities processing transactions of marketplaces that may be abused by criminals to sell or rent stolen goods.

Throughout 2020 and 2023 the CRF received almost 200 reports with regard to robbery and theft and 3 reports with regard to illicit trafficking of stolen goods. Overall, it should be noted that it is quite challenging to differentiate whether a used good has been legitimately sold by the proper owner or whether it has been a stolen good. This is especially true for low-value objects (especially those with no serial number or other indicators enabling the proper identification of a good) or hard to trace goods such as precious metals and stones. In the same period, judicial authorities received 120 MLA requests with regard to "robbery and theft" and 20 MLA requests considering "illicit trafficking in stolen and other goods". Nonetheless, it should be noted that the Grand-Ducal Police cites robbery as top-five crime area with regard to incoming and outgoing requests through the Europol's secure information exchange network.

#### *5.1.9.4. Trafficking in human beings and migrant smuggling*

Although analysed together for the purpose of this risk assessment, it should be noted that human trafficking and migrant smuggling have distinct aspects. For instance, the smuggling ends with the arrival of the migrant in the destination, whereas human trafficking often involves ongoing exploitation in some other way. Moreover, migrant smuggling is always transnational whereas human trafficking may not be[136]. Nevertheless, trafficking in human beings and migrant smuggling are often linked with other forms of

[136] FATF, *ML/TF Risks Arising from Migrant Smuggling*, 2022, link.

organised crime such as drug trafficking, sexual exploitation, extortion, document fraud, payment card fraud or money mules (cf. CEF), property crimes, cybercrime and other[137].

Europol cites the misuse of legal persons as a frequently encountered mean to obscure activities related to human trafficking and migrant smuggling. They are used as front organisations for ML, exploitation of victims, or to obtain documents enabling individuals to enter or stay in the EU. In a similar vein, technologies and the online environment are used to advertise the criminals' services and to recruit facilitators, irregular migrants and potential victims. Applications of AI may deliver new opportunities for criminals to lure potential clients and victims of trafficking in human beings. Disinformation campaigns and deepfakes can be employed to mobilise irregular migrants and increase demand for the services of migrant smugglers[138].

The number of persons vulnerable to trafficking in recent years has increased due to an unprecedented rise in irregular migration and the number of displaced persons, often caused by armed conflict or terrorist organisations controlling territory. According to the Global Peace Index 2024, there were 56 active conflicts in March 2024. This is the most since the Second World War[139]. Trafficking flows related to armed conflict can include human trafficking within and into conflict-affected areas for the purposes of sexual exploitation and forced labour, as well as transnational trafficking flows linked to migrant smuggling[140].

*Human trafficking*

The European Council reports that most common forms of trafficking of human beings in the EU consist in labour exploitation and sexual exploitation[141]. Globally, profits are estimated at EUR 29,4 billion in a single year[142]. Trafficking in human beings is often linked with other forms of organised crime such as migrant smuggling. Furthermore, the threat stemming from human trafficking has been flagged by two of Luxembourg's neighboring countries in their recent national ML/TF risk assessments. Europol notes that crypto assets are used by human traffickers to collect, move and launder illicit profits[143].

*Migrant smuggling*

According to a Europol 2023 report on migrant smuggling "the market for migrant smuggling services to and within the EU is reaching new heights, fuelled by emerging and deepening crises, most notably economic recessions, environmental emergencies caused by climate change, as well as conflicts and demographic pressure in many origin countries"[144]. The FATF report on Migrant Smuggling notes that due to the opaque nature of the crime, as well as the predominant use of cash, it is not possible to produce accurate estimates of global income derived from migrant smuggling. Nevertheless, based on the

[137] European Commission, Together Against Trafficking in Human Beings, link retrieved on 15 December 2022.

[138] Europol, *Tackling threats, addressing challenges Europol's response to migrant smuggling and trafficking in human beings in 2023 and onwards*, 2024, link.

[139] Institute for Economics & Peace, Global Peace Index 2024, link.

[140] FATF - APG, *Financial Flows from Human Trafficking*, 2018 , link.

[141] European Council, the EU's fight against organised crime, link retrieved on 15 December 2022.

[142] European Council, the EU's work to combat human trafficking, link retrieved on 10 April 2024.

[143] Europol, *Tackling threats, addressing challenges Europol's response to migrant smuggling and trafficking in human beings in 2023 and onwards*, 2024, link.

[144] Europol, *Criminal networks in migrant smuggling*, 2023, link.

estimates produced, the total proceeds generated are projected to be in excess of USD 10 billion a year[145]. In its latest report on this matter, Europol confirms that cash payments still prevail as the preferred means of payment in migrant smuggling. Nonetheless, cryptocurrencies are becoming more popular among migrant smugglers[146].

The two case studies below evidence how Luxembourg, and more particularly its financial centre, may be exposed to the external threat in relation to human trafficking and migrant smuggling.

**Case study 7: External threat – human trafficking and migrant smuggling[147]**

An SAR has been filed [with the CRF] regarding 69 transactions made between May 2019 and September 2020, totaling USD 21 300, and suspected to be related to human and/or sex trafficking activities involving one potential perpetrator, six potential victims and three individuals, whose roles were unclear at the moment of filing the SAR.

Suspicions that the transactions and the concerned individuals could be associated with possible human and/or sex trafficking were raised based on the transactional behavior and shared payments instruments. More precisely, connections between the abovementioned individuals could be established based on either connected payment instruments, names, devices, phone numbers, email addresses, IP addresses and other identification details provided to the reporting entity. Additionally, the potential victims were identified due to cross-matches made between phone numbers and female escort advertisements in Southeastern Europe. Moreover, rather than submitting a full picture of the official ID document, subjects only provided a screenshot of the photograph on the ID cards, meaning that the individuals were most probably not in possession of their ID cards. Furthermore, it appeared that one identified individual was already known by the reporting entity for being potentially connected to human trafficking.

Based on the information received, the CRF informed the relevant homologues about the findings. The information provided by the CRF was highly appreciated as further links and evidence were gathered in this way. The intelligence gathered in this case provides certainly only part of the modus operandi of the criminal network, but it is considered to be relevant to lead to potential new perpetrators or victims and identify payment instruments, which could lead to further financial information. In this case the funds were mainly transferred by credit cards. The main financial indicators were the shared payments instruments.

[145] FATF, *ML/TF Risks Arising from Migrant Smuggling*, 2022, link.

[146] Europol, *Tackling threats, addressing challenges Europol's response to migrant smuggling and trafficking in human beings in 2023 and onwards*, 2024, link.

[147] Case study provided by the CRF.

**Case study 8: External threat – human trafficking and migrant smuggling[148]**

The CRF received information regarding individuals potentially involved in the smuggling and/or human trafficking of victims from South America. Most of the perpetrators were EU citizens but with their original birthplace being in various South American countries. While there were some victims without official ID, the majority of victims were holders of a passport from a South American country. The links between the perpetrators and victims were made as they used shared payment instruments, as credit cards, bank, as well as e-money accounts and phone numbers. The perpetrators booked properties online in which they are suspected to have forced the victims to commit sex work as shown by multiple indicators. These indicators include, inter alia, the visits of different men in a short interval of time or sexual services offered by contacting the phone numbers.

Based on the information received, further analysis about transactional and behavioral data were conducted. Additionally, information was requested at different payment entities in Luxembourg leading to new IP and postal addresses, as well as other financial transactions that were relevant to the case. Upon sharing this information with other FIUs it became clear that the victims were likely smuggled from South America to one EU country where the perpetrators reside while they were sent to other countries in the EU to perform sex work.

The information helped to identify the potential perpetrators of a migrant smuggling and human trafficking network, where mostly only the victims were known. Perpetrators used illegal funds on renting of real estate properties, and victims were suspected of being abused for prostitution. The main indicators in this case were the shared payments instruments, as well as the use of money transfers through money remittance providers.

Between 2020 and 2023, the CRF received more than 100 reports in relation to human trafficking and migrant smuggling. In this context, it should be noted that the actual number might be higher, as reports related to sexual exploitation and suspected human trafficking are typically classified as "sexual exploitation". Most (almost 90%) of these reports were filed by entities operating online[149]. As noted throughout the threat assessment and as evidenced in the above case studies, for most of the times, the only link with Luxembourg is the European headquarter of the entity processing relating payments, as well as the Luxembourg account. During the same time, judicial authorities received 16 MLA requests in this respect.

[148] Case study provided by the CRF.

[149] Please note that throughout section 5, the definition of "entities operating online" refers to the one included in the CRF's annual reports (section 2.1.2 *prestataires en ligne*) and encompasses PIs, EMIs, VASPs, and banks operating online. The CRF's annual reports can be accessed here: link.

### *5.1.10. Analysis of external predicate offences: low and very low threat exposure*

The following table resumes the predicate offences that were assessed to bear a lower threat level.

**Table 10: External threat assessment, low and very low threat levels**

| | Likelihood/ probability | Size/ proceeds | External threat level |
|---|---|---|---|
| **Illicit arms trafficking** | Low | Low | Low |
| **Environmental crime** | Low | Low | Low |
| **Extortion** | Low | Low | Low |
| **Murder, grievous bodily injury** | Low | Low | Low |
| **Kidnapping, illegal restraint and hostage taking** | Low | Low | Low |
| **Counterfeiting currency** | Low | Low | Low |
| **Piracy** | Low | Low | Low |

Illicit firearms trafficking is one of the EU's priorities in the fight against serious and organised crime as part of EMPACT 2022-2025. Europol notes that arms trafficking occurs on a small scale and that trafficked weapons are almost exclusively a supplementary rather than a primary source of income for the small number of organised criminal groups involved. Weapons trafficked are intended for either personal use or to meet specific orders[150].

Illegal firearms and their parts have been traded online via the surface and dark web and distributed using post and parcel services for some time. The online sale of illegal firearms appears to have shifted away from dark web marketplaces to forums and other platforms after a number of marketplaces banned the sale of firearms. However, the scale of the online trade in illegal firearms has been assessed as limited compared to their offline supply. In addition, many offers for illegal firearms online are believed to be scams[151]. This being said, Luxembourg authorities confirmed that cases relating to this predicate offence are rather limited (in likelihood and generated proceeds). It has, therefore, been decided to lower the associated threat level from "Medium" in the 2020 NRA to "Low".

With regard to environmental crime, it should be noted that it is also one of the EU's priorities in the fight against serious and organised crime as part of EMPACT 2022-2025. Furthermore, the FATF 2022-2024 Presidency aimed to raise ML/TF awareness in relation to environmental crime. Although figures provided by Luxembourg authorities are rather low with regard to this particular crime, it should be noted that global reports, such as the FATF Report on Money Laundering from Environmental Crime, estimates that environmental crime is suggested to be among the most profitable proceeds-generating crimes in the world[152].

[150] Europol, Illicit firearms trafficking, link retrieved on 9 April 2024.
[151] Europol, *Serious and organised crime threat assessment (EU SOCTA)*, 2021, link.
[152] FATF, *Money Laundering from Environmental Crime*, 2021, link.

**Insight Box 11: Environmental crime[153]**

Generally, the term "environmental crime" covers the gamut of activities that breach environmental legislation and cause significant harm or risk to the environment, human health, or both. These offences can include, but are not limited to the:

- improper collection, transport, recovery or disposal of waste;
- illegal operation of a plant in which a dangerous activity is carried out or in which dangerous substances or preparations are stored;
- killing, destruction, possession or trade of protected wild animal or plant species; and
- production, importation, exportation, marketing or use of ozone-depleting substances.

Waste trafficking demonstrates the extent of the problem. The use of legal business structures by criminal actors are an inherent feature of this crime area. In many cases, criminal actors and legal businesses are indistinguishable. As part of this development, criminals involved in waste trafficking have moved towards the more complex business model of illicit waste management rather than simply illegally dumping waste.

Waste traffickers now operate along the entire waste-processing chain and rely heavily on the use of fraudulent documents.

## 5.2. Domestic exposure: money laundering of proceeds of domestic crimes

The threat from ML of proceeds of domestic crimes is estimated to be smaller (overall moderate) than that from foreign crimes. This is due to Luxembourg's low crime rate.

The Organised Crime Portfolio[154] estimates that the aggregate revenue across a set of illicit markets (i.e. drug trafficking, fraud, counterfeiting, theft) in Luxembourg is around EUR 161 million (i.e. around 0,4% of GDP), which is lower than for neighbouring countries (France: around EUR 16 billion or 0,8% of GDP; Germany: around EUR 17 billion or 0,7% of GDP; and Belgium: around EUR 2,5 billion or 0,7% of GDP), and close to half the estimate for the EU as a whole (i.e. 0,9% of GDP on average). Moreover, Luxembourg's ranking of particular factors by the Rule of Law Index 2023 suggests that the domestic level of crime is rather low: 1$^{rst}$ in order and security, 8$^{th}$ in absence of corruption, and 13$^{th}$ in criminal justice (out of 142 countries)[155].

However, the Grand-Duchy's wealth, its economy, its high number of international institutions and its central location in Europe increase the threat level for certain crimes. While some crimes might be perpetrated domestically, this does not necessarily imply that their proceeds are exclusively laundered in the Grand-Duchy. Considering the border control-free Schengen Area, illicit proceeds might be taken

[153] Europol, Environmental Crime, link retrieved on 6 August 2024.
[154] Organised Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organised Crime in Europe*, 2015, link.
[155] World Justice Project, Rule of Law Index 2023, link.

abroad (e.g. offences committed by foreign organised crime groups, taking robbed goods or proceeds outside Luxembourg).

The following table summarises the level of likelihood/probability, size/proceeds, consequences and overall domestic threat level for every ML-related predicate offence.

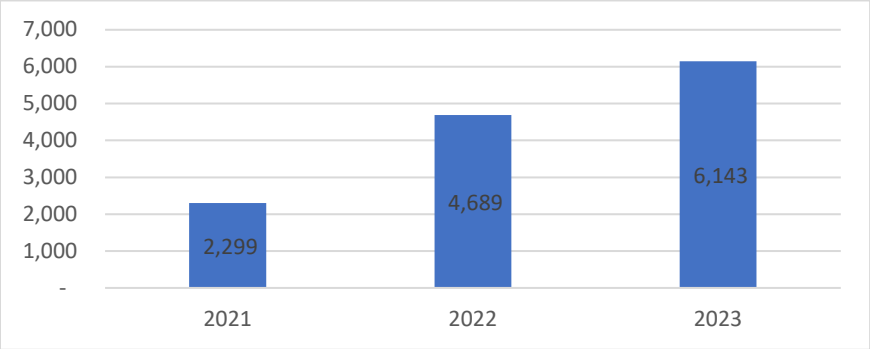
**Table 11: Domestic ML threat level, breakdown per predicate offence**

| Predicate offence | Likelihood/ probability | Size/proceeds | Consequences | Domestic threat level |
|---|---|---|---|---|
| Fraud and forgery | High | High | High | High |
| Robbery and theft | High | High | Medium | High |
| Drug trafficking | High | Medium | High | High |
| Cybercrime | Medium | Medium | High | Medium |
| Sexual exploitation, including sexual exploitation of children | Medium | Low | High | Medium |
| Tax crimes | Medium | Medium | Medium | Medium |
| Corruption and bribery | Medium | Medium | High | Medium |
| Participation in an organised criminal group and racketeering | Medium | Low | High | Medium |
| Trafficking in human beings and migrant smuggling | Low | Low | High | Medium |
| Extortion | Low | Medium | Low | Low |
| Illicit trafficking in stolen and other goods | Low | Low | Low | Low |
| Illicit arms trafficking | Low | Low | Low | Low |
| Insider trading and market manipulation | Low | Low | Medium | Low |
| Environmental crimes | Low | Very Low | Medium | Low |
| Smuggling | Low | Low | Low | Low |
| Counterfeiting and piracy of products | Medium | Very Low | Low | Low |
| Murder and grievous bodily injury | Very Low | Very Low | High | Low |
| Kidnapping, illegal restraint and hostage taking | Very Low | Very Low | High | Low |
| Counterfeiting currency | Low | Very Low | Low | Very Low |
| Piracy | Very Low | Very Low | Low | Very Low |

### 5.2.1. *Fraud and forgery*

The Grand-Ducal Police notes in its annual reports an increase in activities related to fraud, especially with regard to CEF.

**Figure 10: Number of registered cases with the Grand-Ducal Police, 2021-2022**[156]




The number of cases registered for "fraud" by the Grand-Ducal Police is the second highest after theft (i.e., *"vols simples"*). In this context, it is also interesting to note that in 2022, the number of registered cases has more than doubled, from 2 299 cases in 2021 to 4 689 cases in 2022. In 2023, the number of registered cases continued to increase, but to a lesser extent (increase of +31%).

#### 5.2.1.1. *Cyber-enabled fraud*

As noted in the external threat assessment on fraud and forgery, CEF is globally on the rise. Digitalisation and the development of new technologies serve as key drivers underpinning the scale, scope and speed of CEF. With regard to section 5.1.1.1, CEF is indeed a transnational threat where victim and perpetrator do not have to be necessarily located within the same jurisdiction. Luxembourg is, therefore, no exception. Hence, general observations outlined within section 5.1.1.1 apply therefore equally to the Luxembourg context. As noted in section 3, Luxembourg residents engage in online activity and use the internet for a broad range of services, such as online banking, public services, or online shopping. Considering Luxembourg's connectivity rate and the number of residents participating in such activity, criminals may exploit these factors to commit CEF.

The Grand-Ducal Police confirms in its annual reports that they are increasingly confronted with illicit banking activities, phishing and investment scams related to crypto assets. Perpetrators contact victims remotely via social media and convince them to "invest" considerable amounts of money in virtual assets without ever yielding the promised returns. The anonymity offered by the internet combined with the inherently transnational nature of crypto assets and the protection of non-cooperative countries hamper prosecution[157]. Europol confirms indeed that investment fraud generates millions of illicit profits and crypto assets remain the most reported product offered to victims in this type of fraud[158].

[156] Police Grand-Ducale, Chiffres de la délinquance 2022 et 2023, link and link.
[157] Police Grand-Ducale, *Rapport d'activités 2023*, link and Police Grand-Ducale, *Rapport d'activités 2022*, link.
[158] Europol, *Internet organised crime threat assessment (IOCTA) 2024*, 2024, link.

**Case study 9: Phishing scam, money mule and crypto[159]**

A first report was filed with the CRF by a local retail bank indicating that based on their transaction monitoring unusual incoming wire transfers have been observed on individual A's bank account. The suspicions raised were based on two main indicators (1) multiple incoming wire transfers that occurred the same day (2) amounting to approximatively EUR 50 000, which was not in line with the customer profile.

The incoming wire transfers came from another Luxembourg bank account held by individual B having no apparent link to individual A.

Subsequently, a total of EUR 40 000 was transferred out to a Liechtenstein bank account, unknown by the local retail bank at that time, and EUR 9 800 were withdrawn with individual A's credit card.

A few days later, a second report was filed by another local retail bank indicating that the account holder B has become victim of a phishing fraud. The victim received a fraudulent message via telephone falsely claiming to be from Luxembourg's local digital identity independent trusted provider. The message required the victim to take an urgent action to renew the digital identity certificate, to click on a link and share personal credentials on a phishing website. In addition, the victim received a call from an individual pretending to be from his bank, informing the victim that his bank account was hacked and that the access to the e-banking platform was temporarily suspended, which gave the criminals the necessary time to organise the outgoing transfers.

An international information exchange has been initiated by the CRF in order to follow the money trail and secure the funds transferred under fraudulent pretenses to Liechtenstein. It turned out that the beneficiary Liechtenstein bank account was a dedicated bank account of an Luxembourg registered VASP used to safekeep all fiat funds that their customer deposit with the VASP to fund their "crypto" trading activities. The CRF then reached out to the local Luxembourg VASP in order to have clarifications about the identity of the holder of the trading account and about the money trail of the EUR 40 000.

Subsequently, the identified trading account and the Luxembourg bank account held by individual A were frozen, meaning that individual A could neither trade nor withdraw any fiat or virtual assets. Based on the swift actions taken at all levels and the excellent cooperation between the reporting entities and the FIUs, the funds which had already been converted in 25,50 Ethereum could be secured.

Based on additional intelligence gathered, it turned out that individual A was recruited by criminals in a bar offering individual A a commission for receiving and transferring funds. More precisely, the criminals asked individual A to give them the two factor identification codes in order to gain access and take control over his bank account. In addition, the criminals asked for the credit card and made a photo of individual A's ID card, as well as a photo of him. These identification items allowed the

[159] CRF.

criminals to open a trading account with the VASP in the name of individual A and to have full access to it.

It is assumed that the criminals recruit money mules, who accept to receive and transfer funds in return of a commission, and use these money mule bank accounts to defraud phishing victims. By using local bank accounts, criminal increase their success rate, as the victims are less vigilant.

Criminals constantly adapt their modus operandi to exploit potential vulnerabilities and loopholes. For instance, the Grand-Ducal Police noted in 2020 that ransomware attacks increasingly targeted businesses and professionals to exploit vulnerabilities arising from the rapid transition to remote working. As these attacks have decreased following the adaptation of businesses' IT systems in 2021, the Grand-Ducal Police observed that criminals tailored phishing campaigns to users of some Luxembourg online banking services and the national public portal "guichet.lu" in 2023. In a similar vein, the CRF notes that throughout 2022, the number of filings made by some banks has increased as some of their clientele fell victim to these attacks. Overall, it should be noted that amounts involved and techniques used by fraudsters are evolving, as criminals adapt their modus operandi constantly. In 2023, following massive awareness raising campaigns on the modus operandi of these phishing campaigns from the Grand-Ducal Police, supervisors, FIs and the CRF, it has been observed that some of these groups no longer act remotely, but were sent to the victims' homes. These actors were, most of the times, recruited locally and via social media networks to recover credit card information or steal valuables using false pretenses and/or identities.

The Grand-Ducal Police also noted that an increasing number of Luxembourg residents were targeted by so-called "Hi Mum" and "grand-son" scams and some of the related proceeds were laundered via money mules or vIBANs as outlined in the case studies below (cf. see Insight Box 2 for an in-depth explanation on vIBANs).

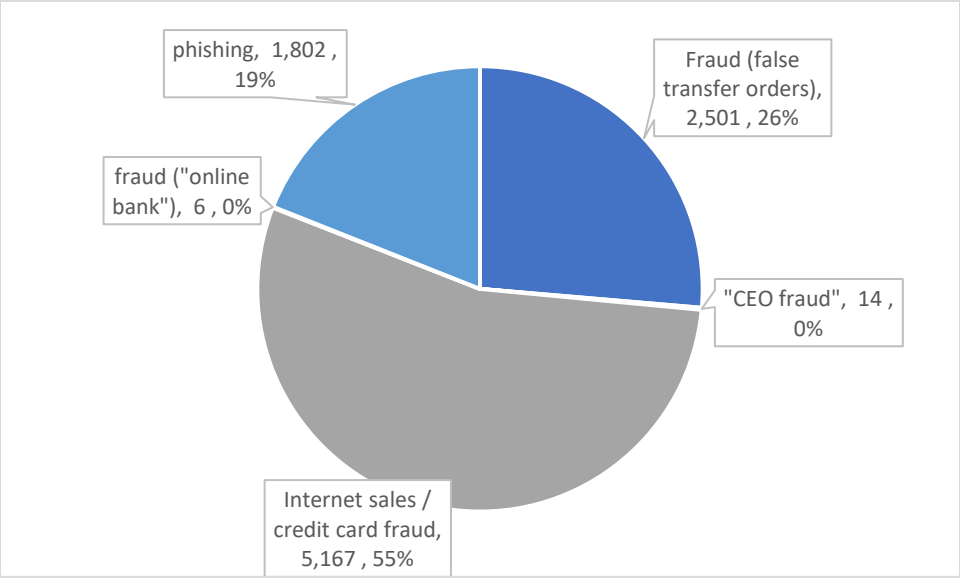
**Case study 10: vIBAN abused for CEF**

Between February and March 2023, the CRF received several reports of so-called "Hi Mum" Scams, where victims received WhatsApp messages from an unknown but local phone number from fraudsters pretending to be their child. The victims received text messages in Luxembourgish via Luxembourg mobile phone numbers, with the inclusion of a Luxembourg IBAN. During the investigation of this case, the CRF discovered that the IBANs provided by the fraudsters were vIBANs. These vIBANs were issued by a Luxembourg banking institution to a Luxembourg based EMI who offered credit cards to European customers[160]. These credit cards can be loaded by transferring money to the vIBANs, which the criminals intended to use for further laundering. Of the six identified vIBANs used in the scam, the CRF was able to block or recall EUR 40 000 out of EUR 55 000 defrauded funds. The CRF's action was facilitated by the co-operation with the bank issuing the vIBANs, which made it possible to quickly identify the PI holding the underlying account of the end customer.

[160] At the date of approval of this report (28 April 2025), the EMI does not offer this service anymore.

In a similar vein, Luxembourg judicial authorities indicated in their annual report that CEF has increased continuously between 2020 and 2023. The following chart depicts the different types of CEF that occurred throughout the observation period and shows that for more than a half, CEF occurs through internet sales and/or involve credit card fraud[161].

**Figure 11: Number of cases per type of fraud, 2020 - 2023[162]**




The FATF-EGMONT report on illicit financial flows from cyber-enabled fraud notes that indeed the location in which the CEF occurs (i.e., where the victim is) is frequently different from the location where the laundering of CEF-proceeds takes place, and money mule networks may span across multiple jurisdictions. It further precises that regions that are highly cashless and digital-based (e.g. where the bulk of financial intermediation is done via online services) are expectedly more vulnerable to the ML risks associated with this crime, although the transnational nature of CEF means that criminals can easily target victims regardless of international borders[163].

#### *5.2.1.2. Luxembourg's domestic threat exposure*

Throughout the observation period of the NRA, judicial authorities have received over 1 700 cases in relation with fraud and forgery and convicted over 700 criminals to prison sentences[164]. The Grand-Ducal Police notes that fraud and forgery generate, together with drug trafficking, the most important proceeds in Luxembourg. Furthermore, the Grand-Ducal Police cites fraud as top-five crime area with regard to outgoing and incoming requests through the Europol's secure information exchange network. The CRF transferred over 500 cases with respect to fraud and forgery to the State Prosecutors. This represented more than half of all CRF's disseminations to the State Prosecutors during that period. In a similar vein, it

[161] Justice, *Rapport des juridictions judiciaires 2023,* link.
[162] Justice, *Rapport des juridictions judiciaires 2023,* link.
[163] FATF – Interpol - Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud*, 2023, link.
[164] It should be noted that this figure includes the number of suspended prison sentences.

should be noted that this crime category encompasses a wide array of criminal offences, as laid out in Appendix A.

Considering the above, domestic threat related to fraud and forgery is assessed to be "High".

### 5.2.2. *Robbery and theft*

From a statistical point of view, thefts *("vols simples"*) is the most encountered predicate offence considering the number of registered cases with the Grand-Ducal Police (representing around 20% of all predicate offences registered)[165].

Although not exhaustive, there are in general two types of active actors.

- Local actors: these individuals are often homeless or drug-addicts and commit robbery and/or theft in order to finance their survival or addiction. Generated proceeds are rather low (mobile phones, wallets, money, bikes) compared to other offences.
- Organised crime actors operating from abroad: These actors are believed to target Luxembourg due to its wealth (highest real GDP per capita in the EU[166]) and proximity to three borders, giving an impression of an easy escape. Based on experience from LEAs, foreign perpetrators targeting Luxembourg for robberies and thefts come from a variety of locations. Throughout the observation period, these groups have committed attacks on ATMs (amounting to a total of 8 explosions between 2020 and 2023), armed robberies, burglaries, and vehicle related thefts (luxury vehicles and high-end SUVs). In 2021 and 2022, there also appears to be a considerable number of thefts and burglaries committed by repeat offenders that are minors.

#### 5.2.2.1. *Luxembourg's domestic threat exposure: robbery and theft*

Throughout the observation period of this NRA, judicial authorities have received almost 5 000 cases in relation with robbery and theft and convicted over 1 500 criminals to prison sentences[167]. The Grand-Ducal Police cites robbery as top-five crime area with respect to incoming and outgoing requests through the Europol's secure information exchange network.

Considering the above, the domestic threat level for robbery and theft is assessed to be "High".

### 5.2.3. *Drug trafficking*

Luxembourg is exposed to the domestic threat of drug trafficking through various factors:

- The border-free Schengen Area and its proximity with countries estimated to have sizeable drug trafficking activities and markets (e.g. France, Belgium, Germany and Netherlands);
- Europol reports that authorities observed a trend towards trafficking larger individual consignments via sea by exploiting containers passing through global logistic hubs[168]. The

[165] Police Grand Ducale, *Chiffres de la délinquance,* link (years: 2021 – 2023).

[166] Eurostat, Real GDP per capita, link retrieved June 2022.

[167] It should be noted that this figure includes the number of suspended prison sentences.

[168] European Monitoring Centre for Drugs and Drug Addiction and Europol, *EU Drug Markets Analysis: Key insights for policy and practice*, 2024, link.

presence of one of the leading freight airports and a multimodal hub connecting Luxembourg with major European ports could add to this exposition.

#### *5.2.3.1. Luxembourg's domestic threat exposure: drug trafficking*

As per the Grand-Ducal Police, local offenders continue to be particularly active in the local drug market. The situation regarding dealers selling cocaine and marijuana at the Railway Station district in Luxembourg City (street dealing) and the situation regarding dealers near the *"Fixerstuff"* and around the cities located in the South of Luxembourg and the French-Luxembourg border remains unchanged. The 2023 Annual Report of the Grand-Ducal Police noted that traffickers from the Netherlands are also observed to be active in Luxembourg supplying the Luxembourg market with heroin[169]. Judicial authorities noted that issues relating to drug consumption and acquisition have risen in the past years. They also noted an increasing presence of dealers operating within foreign organised crime structures[170].

Luxembourg's customs authority seized throughout the observation period cash stemming from drug trafficking worth EUR 28 939,99. Overall, it should be noted that authorities estimate that cash plays a predominant role in the international and local drug market.

Judicial authorities opened in the observation period over 700 cases linked to drug trafficking, and convicted 670 persons between 2020 and 2023. The Grand-Ducal Police notes that drug trafficking, together with fraud and forgery, generate the most important proceeds in Luxembourg. Furthermore, the Grand-Ducal Police cites drug trafficking as top-five crime area with respect to outgoing and incoming requests to through the Europol's secure information exchange network.

Considering the above, the domestic threat level for drug trafficking is assessed to be "High".

### *5.2.4. Analysis of domestic predicate offences: medium and lower threat exposure*

The following table resumes the predicate offences that were assessed to bear a medium, low or very low threat.

[169] Police Grand-Ducale, *Rapport d'activités 2023*, link.
[170] La Justice, *Rapports des juridictions judiciaires 2023,* link.

**Table 12: Domestic predicate offences: medium and lower threat exposure**

| Predicate offence | Rationale | Likelihood/ probability | Size/ proceeds | Consequences/ impact | Domestic threat level |
|---|---|---|---|---|---|
| **Tax crimes** | Luxembourg legal persons may be misused to commit tax crimes in Luxembourg. Generated proceeds thereof are laundered either in LU or abroad.<br><br>It should, however, be noted that with regard to natural persons, most of the direct taxes are collected throughout the year via withholding by employers.<br><br>With respect to legal persons, electronic filing has been mandatory since 2018, allowing the implementation of a set of technical mechanisms that enable the blocking of automatic taxation and thus triggering a specific review and taxation of legal persons.<br><br>The CRF estimates that about 75% of the total domestic cases are related to direct taxes, with the remaining cases involving either indirect taxes or a combination of both.<br><br>Between 2020 and 2023, Luxembourg direct tax authority (ACD) sent out 209 requests of information to foreign authorities. Most of these requests were addressed to Luxembourg neighboring countries.<br><br>In 2023, most VAT fraud cases in Luxembourg emerged from the automotive sector. Prominently represented were cases involving mobile phones and their accessories (mostly Airpods) or IT components (memory cards, hard disks). Due to intensive cooperation at international level, both commodities have slightly lost in importance and volume over the past 2-3 years. | Medium | Medium | Medium | Medium |

| Predicate offence | Rationale | Likelihood/ probability | Size/ proceeds | Consequences/ impact | Domestic threat level |
|---|---|---|---|---|---|
| | The CRF disseminated 44 cases with regard to suspicions of tax crimes to the State Prosecutors in 2020-2023, most of them relate to domestic cases. | | | | |
| **Cybercrime** | With respect to the Luxembourg's context (cf. section 3), the high level of digital connectivity of Luxembourg may be exploited by criminals. Luxembourg is ranked 4th best connected country in the EU in 2022 and a considerable share of Luxembourg residents use the Internet at least once a week.<br><br>The CRF transferred 8 cases with respect to cybercrime to the State Prosecutors in 2020 - 2023.<br><br>Cybercrime can have consequences on data protection, confidentiality and availability, with important social and economic costs. | Medium | Medium | High | Medium |
| **Corruption and bribery** | The level of domestic criminality related to corruption and bribery is deemed to be relatively low in Luxembourg. The 2023 Corruption Perception Index allocates Luxembourg a total score of 79 out of 100 points (i.e. 9th lowest score among 180 countries)[171]. The World Bank Controls of Corruption Index assessed ranked Luxembourg 8th best country with regard to controls against corruption (out of 193 countries)[172]. Moreover, the Rule of Law Index 2023 ranks Luxembourg 8th (out of 140) by absence of corruption[173]. | Medium | Medium | High | Medium |

[171] Transparency International, *Corruption Perception Index*, 2023, link. Note that a country scoring 100 points, is considered to be very clean. A country scoring 0 points is deemed to be highly corrupt.

[172] World Bank, Data Bank: Worldwide Governance Indicators, Control of Corruption, 2023, link.

[173] World Justice Project, Rule of Law Index 2023, link. Note that the first country in the ranking is presumed to have the lowest degree of corruption in government. The last country in the ranking is presumed to have the highest presence of corruption in government.

| Predicate offence | Rationale | Likelihood/ probability | Size/ proceeds | Consequences/ impact | Domestic threat level |
|---|---|---|---|---|---|
| | Luxembourg is home to a number of European institutions, including the Secretariat of the European Parliament, the Court of Justice of the European Union, the European Investment Bank and some Directorate Generals of the European Commission, the heightened presence of PEPs might increase the likelihood of corruption and bribery. As a result, there are some PEPs residing in Luxembourg, although their absolute number (14 000 EU public officials on the territory) is still relatively low. Nonetheless, this exposure should still be considered.<br><br>Corruption could lead to erosion of trust in economic and political institutions. | | | | |
| **Participation in organised criminal group and racketeering** | In the *Rapports juridictions judiciaires*, judicial authorities noted the presence of foreign groups committing serial burglaries, luxury vehicle thefts, ATM thefts using explosives, "shock calls"[174].<br><br>As noted in its annual reports, the Grand-Ducal Police is aware of organised criminal groups committing predicate offences in Luxembourg (e.g. robbery and theft). Some individuals believed to be affiliated to organised/mafia criminal structures have been identified and their accounts were blocked. This demonstrates that Luxembourg is not spared from the risks associated with organised crime[175].<br><br>The participation in organised crime groups may promote violence, social disruption and an increased cost of living. | Medium | Low | High | Medium |
| **Sexual exploitation** | The Grand-Ducal Police observed in its Annual Report of 2023 the increase of a more discreet practice of prostitution, mainly taking place | Medium | Low | High | Medium |

[174] La Justice, *Rapports des juridictions judiciaires 2023,* link.
[175] Police Grand-Ducale, *Rapport d'activités 2023*, link.

| Predicate offence | Rationale | Likelihood/ probability | Size/ proceeds | Consequences/ impact | Domestic threat level |
|---|---|---|---|---|---|
| **including sexual exploitation of children** | in private locations (e.g. apartments). Advertisements offering escort services published on the internet facilitate the rotation of prostitutes in apartments for limited stays. These individuals continue their activities throughout Europe following the same pattern. South American nationals are more represented among those engaging in paid sexual services.<br><br>The Grand-Ducal Police also noted an increase in the sharing of intimate photos and videos. Victims are led to share such photos on social media, either voluntarily or through deceit or false trust. The perpetrators are minors or adults posing as minors[176].<br><br>The CRF transferred 7 cases with regard to sexual exploitation to the State Prosecutors in 2020-2023.<br><br>Sexual exploitation has a high economic and social cost, with victims subjected to long-lasting physical and emotional impact. It can also have some impact on the attractiveness for business due to the nature of crime and broader concerns around labour exploitation and modern slavery associated with this offence. | | | | |
| **Trafficking in human beings and migrant smuggling** | The Global Organised Crime Index ranked Luxembourg 171th out of 191 for human trafficking (lowest rank in the EU after Finland) and 173th out of 189 for human smuggling (lowest rank in the EU)[177].<br><br>Luxembourg is considered a country of destination and transit for victims of trafficking in human beings[178]. | Low | Low | High | Medium |

[176] Police Grand-Ducale, *Rapport d'activités 2023*, link.

[177] Global OC Index, retrieved on 30 December 2023 link and link. Note that the first ranking is reserved to countries being presumed to have significant level of human trafficking and migrant smuggling.

[178] Group of Experts on Action against Trafficking in Human Beings, *Evaluation Report Luxembourg*, 2022, link.

| Predicate offence | Rationale | Likelihood/ probability | Size/ proceeds | Consequences/ impact | Domestic threat level |
|---|---|---|---|---|---|
| | The most common form of exploitation in Luxembourg is labour exploitation (in the HORECA and construction sectors)[179].<br><br>In 2022, Luxembourg reported 50 identified victims and 15 presumed victims of human trafficking. In 2021, Luxembourg reported 20 identified victims of human trafficking and 30 presumed victims of human trafficking[180]. Judicial authorities noted that the number of cases relating to human trafficking and migrant smuggling have risen[181]. The CRF disseminated 1 case to the State Prosecutors between 2020 and 2023.<br><br>Trafficking in human beings and migrant smuggling generates significant social and human harm. | | | | |
| **Extortion** | As noted earlier, extortion may occur through cyber-enabled crime. The Grand-Ducal Police noted that the number of cases related to ransomware reached its peak in 2020. In these cases, victims were often extorted to pay a ransom in crypto-currency in order to recover their data[182]. | Low | Medium | Low | Low |
| **Insider trading and market manipulation** | The threat level from insider trading and market manipulation is assessed as low due to the low volume and complexity of domestic trading, the type of financial instruments admitted to trading (mostly debt instruments), the likely low proceeds and the enhanced transparency of the activity in Luxembourg (members and participants of the Luxembourg Stock Exchange are exclusively regulated firms). | Low | Low | Medium | Low |

[179] Commission consultative des Droits de l'Homme du Grand-Duché de Luxembourg, *Rapport sur la traite des êtres humains au Luxembourg années 2021-2022,* 2024, link.
[180] Commission consultative des Droits de l'Homme du Grand-Duché de Luxembourg, *Rapport sur la traite des êtres humains au Luxembourg années 2021-2022,* 2024, link.
[181] La Justice, *Rapports des juridictions judiciaires 2023,* link.
[182] Grand-Ducal Police, *Rapport d'activités 2021*, link.

| Predicate offence | Rationale | Likelihood/ probability | Size/ proceeds | Consequences/ impact | Domestic threat level |
|---|---|---|---|---|---|
| | The CRF transferred 3 cases to the State Prosecutors with respect to insider trading and market manipulation during the observation period. | | | | |
| **Counterfeiting and piracy of products** | Factors such as the border control-free Schengen Area coupled with Luxembourg's geographical location, the presence of one of the leading freight airports and a multimodal hub connecting Luxembourg with major European hubs could potentially increase the likelihood that counterfeited and pirated goods are transiting through Grand-Duchy.<br><br>Luxembourg customs authority (ADA) is responsible for customs control and supervision of goods entering or leaving the customs territory of the European Union. The majority of detected counterfeited goods came from China and Hong-Kong and entered Luxembourg via airfreight. Most of these goods were clothes, shoes and *"maroquinerie"* (such as, bags, wallets, belts) intended for private usage of people residing outside of Luxembourg (and within the EU internal market). It should be noted in this context that, with respect to the infringements detected by Luxembourg customs authority, trademark holders are informed of the detected infringements and may decide to file a complaint with judicial authorities.<br><br>It should be noted that similar to the conclusions drawn in section 5.1.6 and considering Luxembourg's online activity (see section 3), online shopping has grown with over 80% of Luxembourg internet users having bought or ordered something online.<br><br>The CRF disseminated 9 cases with respect to counterfeiting and piracy of products to the State Prosecutors between 2020 and 2023. | Medium | Very Low | Low | Low |

| Predicate offence | Rationale | Likelihood/ probability | Size/ proceeds | Consequences/ impact | Domestic threat level |
|---|---|---|---|---|---|
| **Environmental crimes** | Proceeds of environmental crimes (e.g. related to waste management services, emission schemes, environment standards or wildlife) are deemed low due to the small geographical size and population of Luxembourg. Nonetheless environmental/wildlife harm can have long-lasting effects. | Low | Very Low | Medium | Low |
| **Murder, grievous bodily injury** | It is estimated that Luxembourg has a low domestic murder rate. | Very Low | Very Low | High | Low |
| **Kidnapping, illegal restraint, and hostage taking** | There are very few reported cases of kidnapping (54 national cases between 2020-2023), illegal restraint, and hostage taking. These crimes are generally carried out by individuals rather than as a result of organised crime. Hence, there are very little proceeds to be laundered.<br><br>The CRF disseminated one case with regard to kidnapping, illegal restraint and hostage taking throughout the observation period to the State Prosecutors. | Very Low | Very Low | High | Low |
| **Illicit arms trafficking** | Luxembourg ranked among the countries with the lowest arms trafficking rate (ranked as 175th out of 192 for arms trafficking in the Global Organised Crime Index)[183]. | Low | Low | Low | Low |
| **Illicit trafficking in stolen and other goods** | There are few cases in Luxembourg of trafficking in stolen or other goods (e.g. precious metals, gems, cultural goods and radioactive material). | Low | Low | Low | Low |
| **Smuggling** | There is limited smuggling of goods into Luxembourg due to lower domestic prices (for instance on cigarettes, fuel and alcohol) with respect | Low | Low | Low | Low |

[183] Global OC Index 2024, link.

| Predicate offence | Rationale | Likelihood/ probability | Size/ proceeds | Consequences/ impact | Domestic threat level |
|---|---|---|---|---|---|
| | to neighbouring countries. Taking legally purchased goods out of the country is not a predicate offence in Luxembourg. There has been a low number of cases of undeclared cash at borders[184] (cf. section 6.6.2)[185]. | | | | |
| **Counterfeiting currency** | Through the observation period:<br>- Luxembourg ranked 22nd in the EU for counterfeiting currency in 2020-2022 and 25th in 2023. An annual average of 539 banknotes worth EUR 23 865 were detected in Luxembourg[186];<br>- The CRF disseminated 4 cases with regard to counterfeiting currency throughout the observation period to the State Prosecutors. | Low | Very Low | Low | Very Low |
| **Piracy** | Luxembourg has no open sea access and no known river piracy making this predicate offence very unlikely for ML. | Very Low | Very Low | Low | Very Low |

[184] Note that since the entry into force of the 2021 Cash Control Law, there is an obligation to declare cross-border transports of cash when traveling to or from Luxembourg, from or to third countries (extra-EU) and from or to EU Member States (intra-EU). For unaccompanied cash, sent in parcels, containers or freight across the border of Luxembourg, there is a disclosure obligation in place.

[185] CRF data.

[186] BCL data.

## 5.3. Emerging and evolving threats: restrictive measures in financial matters

The Law of 20 July 2022 establishing an interinstitutional committee in charge of monitoring the implementation of restrictive measures in financial matters, within the meaning of the Law of 19 December 2020 on the implementation of restrictive measures in financial matters (the "Law of 19 December 2020") added the failure to comply with such measures, to Luxembourg's predicate offences of ML further to article 506-1 of the penal code. More specifically, failure to comply with the restrictive measures as adopted by way of a grand-ducal regulation pursuant to article 4(1) of the Law of 19 December 2020, or by way of an act by the EU or United Nations pursuant to article 4(2) of the Law of 19 December 2020, shall be punished by imprisonment for a term of eight days to five years and a fine of between EUR 12 500 and EUR 5 million or by one of these penalties only. Where the offence has resulted in substantial financial gain, the fine may be increased to four times the amount of the offence.

Pursuant to article 3 of the Law of 19 December 2020, the adherence to the restrictive measures is a legal obligation that does not only apply to the professionals of the financial sector but to all Luxembourgish natural and legal persons, residing or operating in or through the Grand-Duchy of Luxembourg territory or abroad; to legal persons having their head office, or a permanent establishment or their centre of main interests in the Grand-Duchy of Luxembourg territory and that operate in or through the Grand-Duchy of Luxembourg or abroad; to branches of Luxembourg legal persons as well as to branches of foreign legal persons established in Luxembourg; and to all other natural or legal persons operating in the Grand-Duchy of Luxembourg.

Notwithstanding the limited observation period for the purposes of this assessment (from July 2022 until December 2023), Luxembourg actively monitors this evolving threat considering the geopolitical context as well as the fast-paced environment in which restrictive measures are developing.

Further information on the implementation of restrictive measures can be found on the MoF's website. In July 2023, the CRF also issued via goAML a Typology Report on the Circumvention of Financial Restrictive Measures to all registered persons[187]. The "Financial crime" section of CSSF's website contains as well useful information on this subject. The following is an illustrative case study provided by the CRF.

**Case study 11: Circumvention of financial restrictive measures**

A case of a suspicious sale of shares by a sanctioned individual who indirectly owned more than 50% of the voting shares and of the share capital of an EU-based company was reported to the CRF. This company fully owned two non-EU based companies which both had bank accounts in Luxembourg. The deposits thereon were frozen by the reporting bank which also duly reported it to the MoF under Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine.

The circumstances which triggered the suspicions were changes to the shareholding structure of the abovementioned entities around the time their BO was designated by the EU sanctions list. By an

[187] Note that obliged entities can request a copy of this report via goAML.

amendment agreement to the prenuptial contract between the BO and his spouse, a percentage of his share interest was transferred to his wife.

In addition, a trusted person of the BO purchased a percentage of his shares well below their market value via a sale and purchase agreement ("SPA") a few days prior to the designation. The BO also stepped down from all management positions in the group of companies.

As a result of these changes, the BO stated holding not more than 50% of the shares in the group of companies and that the freeze on the deposits of the two non-EU based companies should thus be lifted.

The following elements were considered as suspicious:

- timing of the transactions,
- shares sold significantly under market value,
- simplistic text and terms of the SPA,
- inconsistency with previous transactions,
- destination of the purchase price etc.

As a consequence, considering the circumstances of the changes made to the shareholding structure of the companies involved, the CRF was not in a position to exclude that the companies remain under the control and ownership of said BO by more than 50%.

Supervision and enforcement activities by supervisors contribute to further mitigate such threats as demonstrated in the case study below.

**Case study 12: Adequate application of European financial sanctions and restrictive measures against Russia and Belarus observed through thematic ad-hoc AML/CFT on-site inspections**[188]

In order to ensure that the professionals comply with European financial sanctions and restrictive measures against Russia and Belarus with respect to the war in Ukraine, a set of thematic on-site inspections was carried out in 2023 with twelve professionals presenting a significant exposure towards Russia/Belarus. In this context, the CSSF verified, in particular, the sound functioning of the name matching system (applied to the customer base payment systems and assets under management), ensured that the processing of the generated alerts was efficient and adequate and verified that the professionals had put in place mechanisms allowing, on the one hand, to verify that the transactions linked to Russia or Belarus did not breach the sanctions specific to certain business areas and, on the other hand, to identify potential circumventions or circumvention attempts of the European sanctions. It also ensured that the professionals have in place controls allowing them to identify potential circumvention of financial sanctions (such as identification of potential strawmen, unjustified changes of BOs, etc.) and verified the proper application of restrictive measures and sound coordination of the professionals with the MoF.

As a whole, these on-site inspections allowed confirming that the professionals addressed financial sanctions with due care. However, in certain cases, professionals blocked transactions but did not

[188] Case study provided by the CSSF.

report them to the MoF or the CRF at all or at a late stage. The CSSF therefore reiterated that where restrictive financial measures are applied, the MoF must be notified without delay.

It also drew the professionals' attention to the risk of circumvention of sanctions, such as through transactions from or to countries that are not subject to European regulations or by changing the role of shareholder to creditor of certain persons likely to appear on the sanctions lists.

# 6. Inherent ML risk- vulnerabilities assessment

As in the 2020 NRA, 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 resulting inherent ML risk levels do not take into account the effects of existing mitigating measures. In fact, the impact of mitigating measures in reducing inherent risks for the different sub-sectors is assessed in the section on mitigating factors.

## 6.1. CSSF supervised sectors

The table below shows the inherent risk outcomes for the sectors falling within the AML/CFT supervision of the CSSF.

In order to account for more granularity, the analysis of the retail and business banks sub-sector encompasses the analysis of both retail and business banks, as well as entities operating online.

Furthermore, VASPs were included within the vulnerabilities assessment, as the Law of 25 March 2020 amending the 2004 AML/CFT Law added VASPs within the scope of the CSSF AML/CFT supervision.

The Law of 21 July 2021 amended the Law of 5 April 1993 on the financial sector (1993 LFS). Taking this into account, the taxonomy and definition of investment firms were adapted.

**Table 13: Inherent ML risk by sub-sectors (CSSF supervised sectors)**

| Sector | Sub-sectors | 2025 NRA: Inherent risk |
|---|---|---|
| Banks | Retail and business banks | High |
| | Entities operating online | High |
| | Wholesale, corporate and investment banks | High |
| | Private banking | Very High |
| | Custodians and sub-custodians (incl. Central Securities Depositories) | Medium |
| Investment sector | Investment firms authorized to carry out the services of investment advice and portfolio management[189] | High |
| | 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[190] | High |
| | 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[191] | Medium |
| | Collective investments | Medium |
| | CSSF-supervised pension funds | Low |
| | Payment institutions (PIs) | High |

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

| Sector | Sub-sectors | 2025 NRA: Inherent risk |
|---|---|---|
| Money value or transfer services (MVTS) | E-money institutions (EMIs) | High |
| | Agents and e-money distributors acting on behalf of PIs/EMIs established in other European Member States | Medium |
| VASPs | | High |
| Specialised PFSs | Specialised PFSs providing corporate services | High |
| | Professional depositaries | Medium |
| Support PFSs and other specialised PFSs[192] | Support PFSs | Very Low |
| | Other specialised PFSs | |
| Market operators | | Low |

### 6.1.1. *Banks*[193]

This sector 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**

Overarching key risk drivers for the banking sector are the sector's size, the risks associated with products and activities, and the volume of transactions/clients handled.

As in the case for the 2020 NRA, private banking activities represent a "Very High" inherent risk level whereas custodians and sub-custodians are assessed to pose "Medium" risk. The remaining banking sub-sectors (i.e. retail and business banks, entities operating online, wholesale, as well as corporate and investment banks) pose a "High" inherent risk.

Luxembourg's banking sector is large in terms of size. The Grand-Duchy counted 120 entities in 2023 from over 20 different countries and managed assets worth around EUR 929 billion in 2023. The criteria "ownership/legal structure" posed high ML risks for the whole banking sector (with the exception of retail and business banks and custodians and sub-custodians), as only around 7% of banks were domestically owned and the remaining were foreign-owned (with about 50% EU and 50% non-EU ownership throughout the observation period).

Vulnerabilities linked to the products and activities were assessed high for the whole banking sector, in line with the 2022 SNRA (see boxes in subsequent sub-sections related to the banking sub-sectors).

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

[193] Please note that the terms "client account" or "clients" refer to number of "client root accounts as defined in the CSSF Financial crime questionnaire (Extract of the "Completion Notes" of the annual survey: "The term "account" refers to the root account number (*Kontostammnummer, racine du compte bancaire*) under which several different sub-accounts (current accounts, FX accounts, loan accounts, custody accounts etc.) may be maintained. Whenever data is collected on the number of accounts, solely the number of the root accounts should be reported and not the number of sub-accounts. Internal technical accounts are exempted from this definition").

#### 6.1.1.1. *Retail & business banks and entities operating online*[194]

**AT A GLANCE**

At the product level (SNRA, NRA)

Products and activities assessed in the 2022 SNRA related to retail & 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 regarding the whole EU:

- ML risks of retail deposits on accounts are assessed "Very high";
- Business loans are, in most cases, not tailored to ML needs given their high-value nature. Furthermore, abusing business loans for ML purposes requires expertise and knowledge. Thus, ML risks are assessed "Medium";
- Consumer credits and low value loans are assessed to bear "Medium" ML risks.

The 2025 NRA assesses associated inherent risk of these products under "products/activities". In the context of Luxembourg retail & business banks and entities operating online, the resulting associated ML 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. They are in most instances equivalent to products and activities related to retail & business banks notably the offer of current accounts. These entities do not offer products and services under the anonymous prepaid card model. However, a bank account is always used for loading the e-money products.

At the sub-sector level (NRA)

In Luxembourg, these sub-sectors' inherent risk level are "High". Whereas the 2020 NRA assessed "traditional" retail and business banks and entities operating online together, this update of the NRA assesses these two types of banks separately in order to account for their specific and diverging characteristics in some dimensions (e.g. international clientele and distribution channels):

- Key risk drivers for retail & business banks identified in the previous 2020 NRA continue to be relevant: sub-sector size (although highly concentrated) and volume, followed by products and activities, international business, and channels.
- ML vulnerabilities associated to size, international business (even though low exposure to high-risk countries), volume of clients and transactions and distribution channels are considered key risk drivers for entities operating online followed by ownership and products and activities.

[194] Some data regarding retail & business banks and entities operating online apply to both sub-sectors. Therefore, the assessment of these two sub-sectors is included in this sub-section.

*Retail and business banks*

Overall, Luxembourg counted nine retail and business banks managing EUR 173,1 billion of assets and generating a total gross income of EUR 8,5 billion as of end 2023[195]. Entities of this sub-sector employed between 2020 and 2022 the largest number of employees among the banking sub-sectors (8 269 in 2020, 8 266 in 2021 and 8 154 in 2022). In 2023, however, employment in the private banking sub-sector (8 299 employees) exceeded the number of employees within the retail and business banks sub-sector (7 785 employees). In this context it should be noted that the number of retail and business banks has decreased throughout the observation period (from 15 entities in 2020 to 9 entities in 2023).

Considering the decreasing and limited number of entities (among which most have a long-standing presence within the country), ML risks related to ownership are assessed to be less significant. The sub-sector became more concentrated with top-five entities generating over 95% of the market's total assets in 2023 (in comparison to almost 90% in 2020).

The number of client accounts remained significant throughout the observation period (more than 1,3 million client accounts in 2023). This said, most account holders were natural persons (about 90% in 2023), which are less vulnerable to ML than legal persons and arrangements and most of their clientele was based in the EU. In fact, on average between 2020 and 2023, only 1,5% of the retail and business banking clientele resided in non-EU countries. As such, 99% of consolidated flows were with European countries and 0,1% of consolidated flows were with high-risk countries in 2023[196].

As this sub-sector offers a range of different products, the following outlines how these could potentially be abused by criminals:

- As already noted in the 2020 NRA, payment service activities carried out by retail and business banks are potentially vulnerable to ML risks, as they can experience layering and extraction techniques used by criminals which are comparatively more sophisticated than in other sub-sectors, for instance, by funding of a product using one method and withdrawal using another. In a similar vein, and as already noted previously (sections 3 and 5.1.1.1), an increasing share of transactions and payments occurs online. In this regard, it should be noted that in Luxembourg, cards constitute the preferred mean of payments for online transactions. Nonetheless, it should be noted that electronic payment solutions and wire transfers are also widely used[197]. Considering this, threats stemming from fraud, and CEF are relevant for retail and business banks;
- Products offered by the sub-sector (i.e. basic financial services) may also be abused by money mules seeking to transfer proceeds out of the banking sector using personal accounts, either scamming, fake banking websites (for example) or through money value transfer services[198];

[195] CSSF data.

[196] As per CSSF internal rating list.

[197] ABBL/CSSF, *Retail banking survey 2023*, link.

[198] 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.

- Business loans give criminal funds an appearance of legitimacy and perpetrators may use criminal funds to reimburse the latter. Criminals may also opt for loan fraud (i.e. using strawmen, false documentation) to transfer funds[199];
- Consumer credits offer less money laundering potential than other financial products, but criminal organisations may use them to finance the purchase of goods and then redeem the loans by cash[200]. According to the ABBL/CSSF Retail Banking Survey, the volume of consumer credits granted by Luxembourg retail banks in comparison to the total volume of credits is limited, representing 4% of total volume of loans granted in 2022[201];
- Criminals may abuse mortgage credits and high-value asset-backed credits to disguise and invest the proceeds of crime by way of real-estate investment. The proceeds are used for deposits, repayments and early redemption of the credit agreement. The 2022 SNRA notes that organised crime organisations have frequently used this method. They are well equipped to provide false documentation and the structure of the mortgage (with third-party involvement) helps them to hide the real beneficiary of the funds. Mortgage credit constitutes an easy way to enable criminals to own several properties and to hide the true scale of their assets. This method is still used for the integration phase (mostly for lower amounts, as it does not require sophisticated operations). However, it is more often used in combination with concealment of the BO of real estate behind a complex chain of ownership.

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 ML risks.

*Entities operating online*

Although the number of establishments in the sub-sector of entities operating online was very limited, with a total number of five entities as of December 2023, they served a considerable number of client accounts (~89 million in 2023). This exposes the sector to ML risks stemming from the volume of clients served, even though most of them (95%) were natural persons. The share of high-risk clients was low decreasing ML risks stemming from clients.

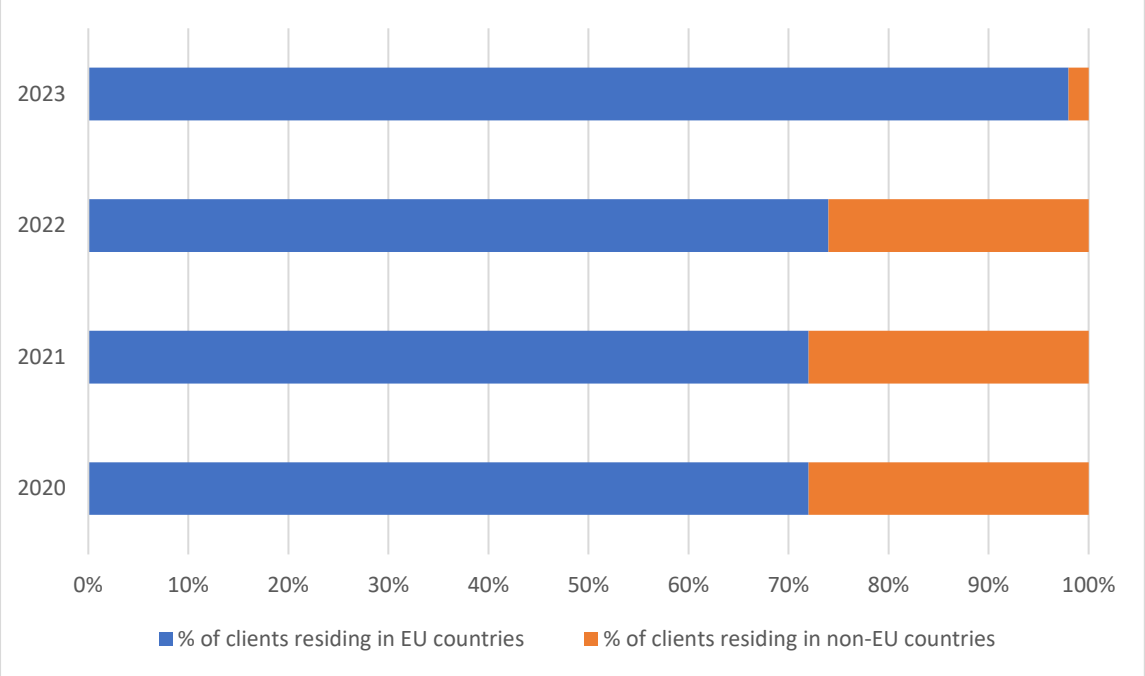
As shown in the graph below, the client-base served by these entities has changed throughout the observation period, and especially between 2022 and 2023. In fact, the arrival of one significant entity explains the volatility relating to the presented figures.

[199] 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.

[200] 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.

[201] ABBL/CSSF, *Retail Banking Survey 2023*, link.

**Figure 12: Breakdown of client residency (entities operating online), indicative data, 2020-2023[202]**




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.

Distribution channels of entities operating online contribute to the ML exposure, as 100% of customers were interacting through online/non-face-to-face channels as the name suggests.

#### *6.1.1.2. Wholesale, corporate and investment banks*

**AT A GLANCE**

SNRA

The 2022 SNRA assesses the corporate banking sector as "High" risk for ML. Key risk drivers identified by the 2022 SNRA are the nature of customers and geographical areas.

NRA

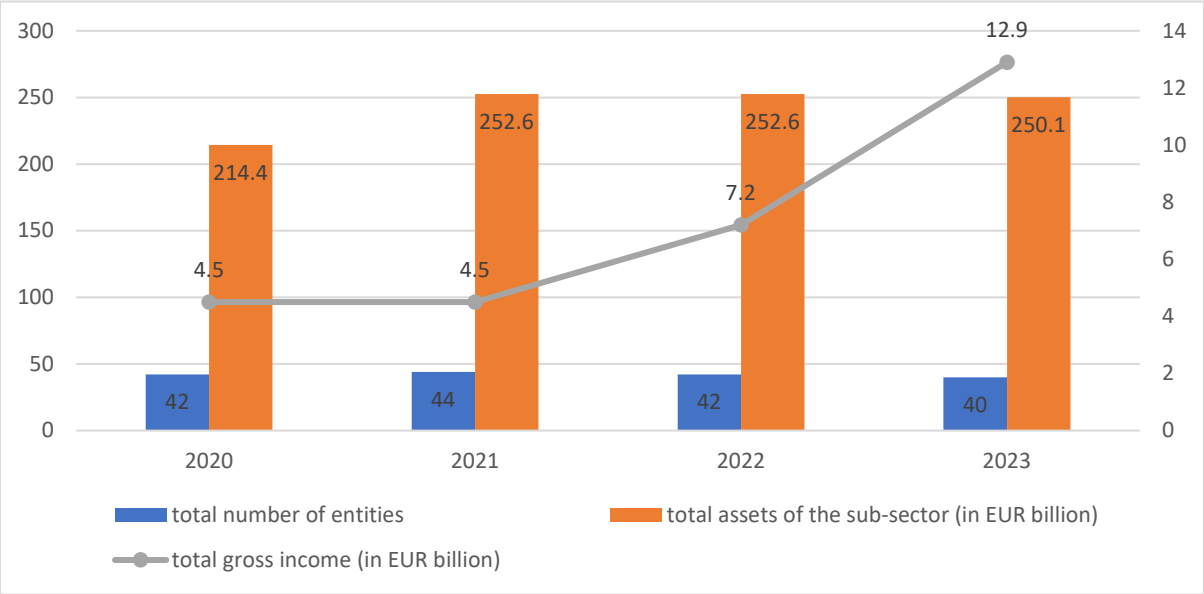
In Luxembourg, the sub-sector inherent risk level remains "High".

Overall, the key risk drivers for wholesale, corporate and investment banks are sub-sector size followed by the sub-sector's fragmentation/complexity, ownership structure, products and activities, international business and clients/transactions (volume and risk).

The sub-sector's size remained more or less stable in terms of number of entities and total assets between 2020 and 2023, as shown in the following figure. Total gross income has, however, increased.

[202] CSSF data.

**Figure 13: Number of entities, total income and assets of wholesale, corporate and investment banks, 2020-2023**




The international nature of the business continued to drive the ML risks of the sub-sector, with 82% of both assets and liabilities related to account holders not based in Luxembourg in 2023. Nonetheless, it should be noted that the sub-sector is mainly oriented towards a European clientele. Indeed, only 17% of clients resided in non-EU countries.

The sub-sector counted a limited number of clients (between 29 000 and 24 000 throughout the observation period). The important volumes and average value per transactions that are processed by this sub-sector as well as the share of high-risk and PEP clients (mostly foreign) increase, however, ML risks with regard to the sub-sector's transaction volumes and client risk.

According to the 2022 SNRA, corporate banking may be exposed to trade-based transactions linked to corporate bank accounts, which could increase ML risk, especially when high-risk jurisdictions are involved. The share of consolidated flows with high-risk countries varied between 0,2% and 1,5% during the observation period[203]. This puts the ML risks exposed in the 2022 SNRA into perspective to some extent.

#### *6.1.1.3. Custodians and sub-custodians (incl. CSDs)*

**AT A GLANCE**

The sub-sector inherent risk level remains "Medium".

Overall, key risk drivers for this sub-sector are sub-sector size, followed by the number (volume) of clients.

[203] As per CSSF internal rating list.

In Luxembourg, the sub-sector consisted of 29 entities resulting in a total gross income of EUR 14,8 billion and assets worth EUR 251 billion in 2023. The sub-sector remained concentrated with top-five entities accounting for more than 70% of the market's assets in 2023.

In 2023, the sector counted around 170 000 client accounts (around 200 000 in 2020), of which 2,5% were flagged as being high-risk. The majority of the sub-sector's clientele were natural persons, although in a decreasing share since 2020. Among the clients that were legal persons (which constitute on average ~25% of the clients), most of the clients 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 doubled in relative terms, which may partly be explained by the decrease of the number of client accounts since 2020.

Custodians' and sub-custodians' clientele resided predominantly in EU countries. Between 2020 and 2023, only 1% of its clientele resided in high-risk countries[204]. The European nature of the business and the limited exposure of the sub-sector to geographies having weak AML/CFT measures limit associated ML risks to some extent.

Services offered by custodians and sub-custodians were mostly commoditised and standardised (e.g. custody of financial instruments, dividend and interests payment collection and distribution). Although ongoing client interaction was indirect, client contact for new account services was direct. Consequently, products and services offered by the sub-sector, as well as the channels used to do so, pose moderate ML risks.

#### *6.1.1.4. Private banking*

**AT A GLANCE**

SNRA

The 2022 SNRA notes that the combination of sophisticated financial services and products, as well as the wealthy customer base often with complex ownership structures, makes the sub-sector highly vulnerable for ML purposes.

NRA

In Luxembourg, the sub-sector inherent risk level remains "Very High".

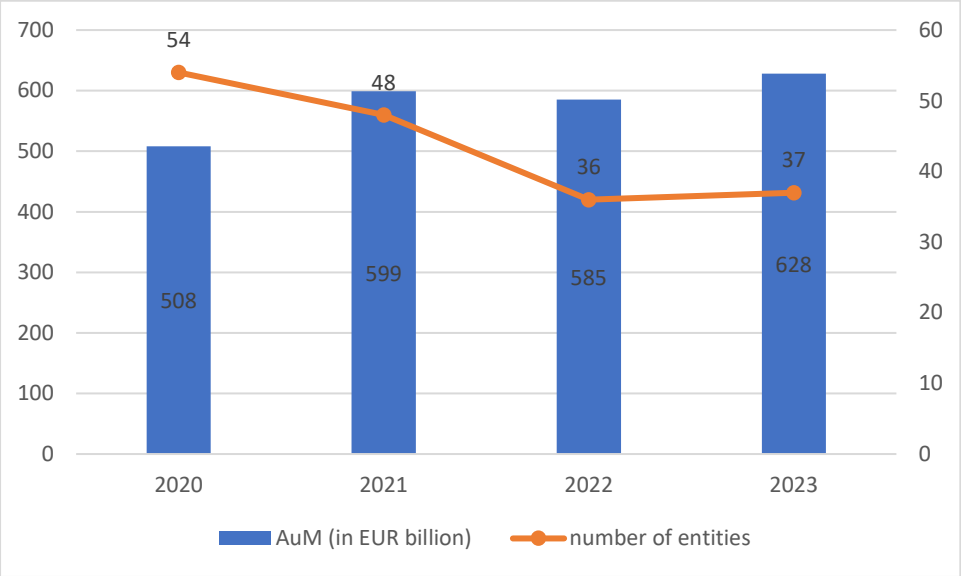
Overall, key risk drivers for this sub-sector are sub-sector size, products/activities and risks related to clients and transactions, followed by sub-sector fragmentation, international nature of business (even though mainly European), clients/transactions' volumes and channels.

- ☞ Please note that the 2023 update of the Private Banking Sub-Sector Risk Assessment on the CSSF's website should be consulted for an in-depth assessment of the private banking sub-sector's ML risks: link

[204] As per CSSF internal rating list.

Luxembourg's private banking sector is large and remained fragmented despite the consolidation process initiated over the past few years. During the observation period, the number of private banking entities has decreased from 54 entities in 2020 to 37 in 2023. Nonetheless, assets under management (AuM) grew substantially.

**Figure 14: Number of entities and AuM in the private banking sub-sector, 2020 - 2023**




The number of clients served by this sub-sector has increased uninterruptedly from 2020 (approximately 166 000) to 2023 (slightly over 191 000). According to the ABBL/KPMG Banking Survey 2024, and their specific scope, about 21% of customers came from Luxembourg, 24% from Belgium, France and Germany and 40% from the rest of Europe[205]. Typical motivations for foreign investors to hold their assets in Luxembourg are the stable political, economic and juridical environment, the strong property protection, the well-regulated and stable financial sector providing numerous investment opportunities, the central European location including membership of the Eurozone, the diverse and high-quality services, the concentration of experts and the international, multi-lingual workforce[206]. The majority of the clientele were natural persons, although a slight shift towards an increasing part of clients being legal persons could be observed (39% in 2020, 41% in 2021, 43% in 2022 and 47% in 2023).

Europe remained the core market of the Luxembourg private banking sector with on average 96% of consolidated flows being with European countries during the observation period. Nevertheless, the share of high-risk clients (on average 10,5% during the observation period) was higher than in other banking sub-sectors (with the exception of wholesale, corporate and investment banks), thereby increasing the ML vulnerability with regard to client risk.

Luxembourg's private banking sub-sector also specialised in specific types of clients, such as affluent or Ultra-High-Net-Worth Individual (UHNW) clients. According to the ABBL Private Banking survey

[205] ABBL/KPMG, *Private Banking Survey 2024*, link.
[206] CSSF, *Private Banking Sub-Sector Risk Assessment (Update 2023)*, link.

2024, clients with assets exceeding EUR 20 million represented around 60% of total AuM throughout the observation period (2020-2023).[207]

Overall, private banking activities can be split into two core categories of asset management services (custody of financial assets, investment services) and four categories of ancillary services (current account banking, credit solution, wealth structuring, insurance solutions). According to the 2023 Private Banking Sub-Sector Risk Assessment, private banks are particularly exposed to the layering and integration stages of ML. Criminals may abuse or misuse sophisticated investment services to obscure the audit trail and sever the link with the original crime. During these stages, funds are typically transferred electronically from one investment or account to another and potentially across several geographies. Eventually, funds are returned in one form or other to the criminal, from what seem to be legitimate sources. The 2023 Private Banking Sub-Sector Risk Assessment also notes that tax crimes, fraud, and corruption and bribery appear as relevant threats for this sub-sector. As access to private banking services is limited and reserved to persons with sufficient funds, large value transactions are likely to occur more frequently in private banking than in other banking sectors, making an unusual and illicit nature of large transfers more difficult to detect and facilitating the introduction of large sums into the financial system.

In general, banks predominantly had physical contact with their clients. However, in private banking, intermediaries such as business introducers, power of attorney and third-party managers were used in addition to the face-to-face contact with the client. This increases the sub-sector's ML vulnerability in relation to channels.

### *6.1.2. Investment sector*

**AT A GLANCE**

SNRA

The 2022 SNRA assesses ML risks linked to the retail and institutional investment sector as "High", with the main vulnerability being the intermediation of services (distribution channels).

NRA

Investment firms (with the exception of investment firms authorized to carry out activities of dealing on own account, of underwriting of financial instruments and/or placing of financial instrument on a firm commitment basis and of placing of financial instruments without a firm commitment basis) are assessed as having high ML risks. Collective investments are assessed as posing moderate ML risks and the CSSF supervised pension funds are assessed as low risk.

#### *6.1.2.1. Investment firms*

The Law of 21 July 2021 amended the 1993 LFS. Taking this into account, the taxonomy and definition of investment firms have been adapted.

- "Investment firms authorized to carry out the services of investment advice and portfolio management" encompasses investment firms having the authorisation for the provision of "portfolio management" (article 24-4 of the 1993 LSF) and "investment advice" (article 24-5

[207] ABBL/KPMG, *Private Banking Survey 2024*, link.

of the 1993 LSF). In the 2020 NRA, this sub-sector was referred to as "wealth and asset managers".

- "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" encompasses investment firms authorized to carry out the services of reception and transmission of orders in relation to one or more financial instruments (article 24-1 of the 1993 LSF) and of execution of orders on behalf of clients (article 24-2 of the 1993 LSF). In the 2020 NRA, this sub-sector was referred to as "brokers and broker dealers".
- "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" encompasses investment firms authorized to carry out activities of dealing on own account, of underwriting of financial instruments and/or placing financial instruments on a firm commitment basis and of placing of financial instruments without a firm commitment basis (article 24-3, 24-6, and 24-7 of the 1993 LSF). In the 2020 NRA, this sub-sector was referred to as "traders/market-makers".

**AT A GLANCE**

Whereas "investment firms authorized to carry out the services of investment advice and portfolio management clients" and "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" pose high inherent risk, "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" pose moderate inherent risk.

Risks related to the sector's products and activities, international business, client/transaction risk and distribution channels impact all investment firms' inherent risk score.

The total number of investment firms decreased slightly during the observation period with 92 entities in 2023 (in comparison to 98 in 2020).

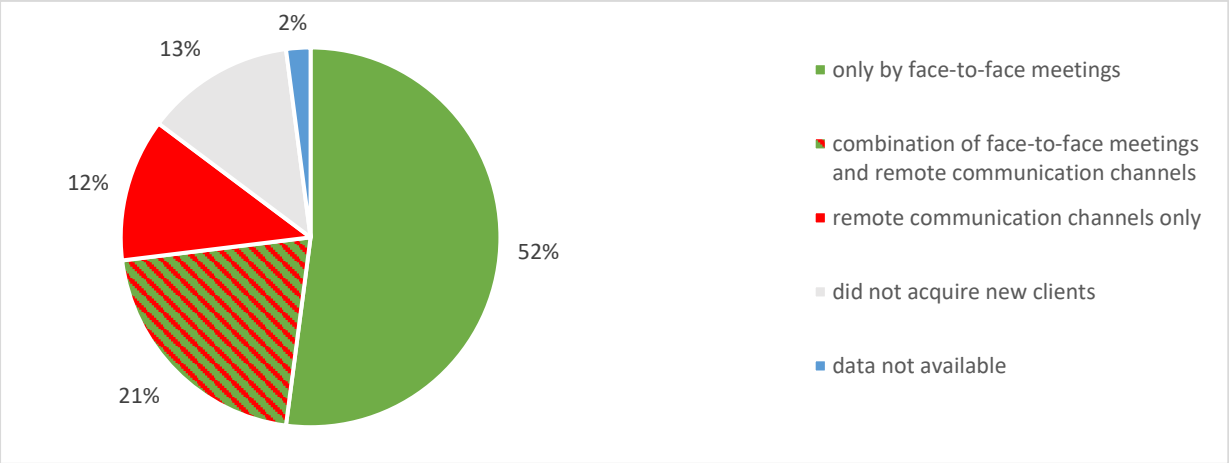
Regarding clients, the number has increased by 51%. This is also mirrored in the number of high-risk clients, which rose by 90% in the same period, representing 4,95% of total client base. Taking this into account, and in comparison to other sub-sectors, ML exposure stemming from clients risk is assessed to be high.

Although investment firms' clientele was mainly made up of natural persons (on average 92% between 2020 and 2023), most clients resided outside of Luxembourg (on average 96%). More precisely, 91% resided in 2023 within the EU and less than 3% in high-risk countries[208]. Considering this, ML vulnerability of investment firms with respect to international business is assessed to be high.

[208] As per CSSF internal rating list.

The following figure presents a breakdown on how clients were acquired in investment firms. Although the majority of investment acquired new clients through face-to-face meetings, about a third of investment firms acquired new clients through remote communication channels.

**Figure 15: Breakdown of client acquisition in investment firms, average figures for 2020 - 2023**




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

**AT A GLANCE**

In the 2025 NRA, investment firms authorized to carry out the services of investment advice and portfolio management remain "High". Key risk drivers are the sub-sector's size, products/activities, international business (analysed above for all investment firms), clients/transactions volume, and client/transactions risk and distribution channels (both analysed above for all investment firms).

This sub-sector encompasses investment firms having the authorisation for the provision of "portfolio management" (article 24-4 of the 1993 LSF) and "investment advice" (article 24-5 of the 1993 LSF). In the 2020 NRA, this sub-sector was referred to as "wealth and asset managers". Whereas the sub-sector counted 91 entities in 2020, there were 84 investment firms with relevant services in 2023:

- 84 investment firms were authorised to carry out the activity of investment advice, with 33 of them exercising those activities. Top-five firms captured nearly 80% of the total revenues, and about 64% of portfolio advised; and
- 73 investment firms were authorised to carry out the activity of private portfolio management, with 65 of them exercising those activities. Top-five firms captured just over half of total revenues, and managed about 62% of AuM.

On average, the entities of the sub-sector had almost 70 000 assigned mandates per year, with 97% stemming from private portfolio management (and the rest from investment advisers). Around seven entities had omnibus accounts and about 21% provided execution services only.

More than half (on average 53%) of the entities were domestically owned, decreasing exposure stemming from foreign ownership. EU and non-EU ownership represented an equal proportion (about 25% each). Most relevant non-EU ownership countries were Switzerland and the USA.

*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*

**AT A GLANCE**

In the 2025 NRA, 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 remain "High". Key drivers are size followed by products/activities, international business (analysed for all investment firms above), client risk (analysed for all investment firms above) and distribution channels (analysed for all investment firms above).

This sub-sector encompasses investment firms authorized to carry out the services of reception and transmission of orders in relation to one or more financial instruments (article 24-1 of the 1993 LSF) and of execution of orders on behalf of clients (article 24-2 of the 1993 LSF). In the 2020 NRA, this sub-sector was referred to as "brokers and broker-dealers".

In 2023:

- Brokers: 88 investment firms were authorized to carry out the activities of reception and transmission of orders in relation to one or more financial instruments, with 33 of them exercising the activity. They generated transactions worth EUR 2 208 billion; and
- Broker-dealers (non-bank): 80 investment firms were authorized to carry out the activity of execution of orders on behalf of clients, with 18 exercising this activity. They generated transactions worth EUR 174,6 billion.

Altogether, the number of assigned mandates within this sub-sector amounted to approximately 77 500 in 2023, slightly above the average of 74 000 observed during the observation period of this NRA. These investment firms processed an impressive number of transactions, both in volume (15 billion) and in value (EUR 2 383,5 billion).

Market fragmentation is assessed to be moderate, as over 60% of the number transactions and over 22% of the volume of transactions were carried out by one investment firm acting as an intermediary in the context of fund distribution between asset managers and sub-distributors. Moreover, this firm exclusively contracted with institutional clients and it did not perform reception and transmission of orders).

Just over half (53%) of the entities were domestically owned during the observation period, decreasing exposure stemming from foreign ownership. EU and non-EU ownership represented an equal proportion (about 25% each). Most relevant non-EU ownership countries were Switzerland and the USA.

*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*

**AT A GLANCE**

In the 2025 NRA, 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 continue to pose moderate ML risk. Key risk drivers are the relative higher foreign ownership, followed by products/activities and the international nature of business (analysed above for all investment firms).

This sub-sector encompasses investment firms authorized to carry out activities of dealing on own account, of underwriting of financial instruments and/or placing financial instruments on a firm commitment basis and of placing of financial instruments without a firm commitment basis (articles 24-3, 24-6, and 24-7 of the 1993 LSF). In the 2020 NRA, this sub-sector was referred to as "traders/market-makers".

In 2023, firms in the sub-sector traded EUR 40,2 billion of assets. As of end 2023, there were seven investment firms providing relevant services. More precisely:

- five investment firms were authorized to carry out the activity of dealing on own account, with three exercising this activity;
- two investment firms were authorized to carry out the activity of underwriting financial instruments and/or placing of financial instruments on a firm commitment basis, with none of them exercising this activity; and
- three investment firms were authorized to carry out the activity of placing of financial instruments without a firm commitment basis, with two of them exercising this activity.

Although the number of mandates has increased continuously between 2020 and 2023, their overall number remained limited, decreasing the related vulnerability to ML risk. Furthermore, no professional carried out the activity of a wealth manager or broker and no broker dealer had omnibus accounts during the observation period.

Out of the seven investment firms authorised to provide the relevant services in 2023, none were domestically-owned. Non-EU ownership remained prevalent throughout the observation period with 71,43% in 2023 increasing the exposure to ML risk. Most relevant jurisdictions were the USA, Switzerland and Monaco.

#### 6.1.2.2. *Collective investments*

**AT A GLANCE**

Collective investments were assessed to bear a "Medium" inherent ML risk. Key risk drivers are the sub-sector structure (in terms of size) and international nature of business.

- ☞ 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 ML risks: link

The below analysis covered Undertakings for Collective Investments in Transferable Securities (UCITS), Management Companies (ManCo) and AIFMs.

Although the number of authorised and registered investment fund managers has slightly decreased from 1 248 as of December 2019 to 1 212 in 2023, net assets of UCIs increased from EUR 4 718 billion in December 2019[209] to EUR 5 285 billion in December 2023[210].

Between 2020 and 2023, around 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 USA (20%), the UK (17%), Germany (15%) and Switzerland (14%), which are considered lower-risk in terms of ML for the origin of the products managed by both UCITs Manco and AIFMs in these countries [211]. Nonetheless, most investors in the collective investment sub-sector were foreign and Luxembourg is characterized by global cross-border distribution of funds.

#### 6.1.2.3. *CSSF supervised pension funds*

**AT A GLANCE**

The sub-sector inherent risk level remains "Low", with no significant change in risk scores with respect to the 2020 NRA.

The ML 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 2023, 11 entities registered as pension funds fell under CSSF supervision. Together, they had EUR 1,26 billion AuM with a yearly average of around approximately 16 000 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 0,023 billion in 2023 (in comparison to 0,665 billion in 2020). In addition, they offer standardised products with low ML risks and had no flows with geographies with weak AML/CFT measures, as most sponsors were EU-based corporates.

[209] CSSF, *Annual Report 2019*, link.
[210] CSSF, *Annual Report 2023*, link.
[211] CSSF, *ML/TF Sub-sector Risk Assessment – Collective Investment Sector (2025 Update)*, link.

### 6.1.3. *Money value or transfer services*

**AT A GLANCE**

At the product level (SNRA, NRA)

The 2022 SNRA assesses ML risks related to payment services. First and foremost, it is to be noted that payment services are not exclusively offered by the MVTS sector but also by the banking sector (see section 6.1.1.1). The 2022 SNRA concludes that ML risks of payment services are high considering their cash-intensive nature, the prevalence of occasional transactions on established business relationships, the large volume and speed of transactions, the possible involvement of high-risk jurisdictions in which entities operate and the use of new technologies to facilitate the onboarding of customers remotely as well as the distribution channels used.

On top of the risks associated with payment services, the 2022 SNRA also analyses ML risks linked to transfers of funds and money remittance. Due to their ease of use, the 2022 SNRA considers the latter as bearing high ML risks.

Within the scope of the 2025 NRA, risks related to products and services of the MVTS sector were assessed under the "products/activities" dimension.

At the sub-sector level (NRA)

In Luxembourg, MVTS inherent ML risk levels remain overall the same as the 2020 NRA levels. Whereas the inherent risk level for both PIs and EMIs remains "High", agents and e-money distributors acting on behalf of PIs/EMIs established in other EU Member States continue to pose a moderate ML inherent risk.

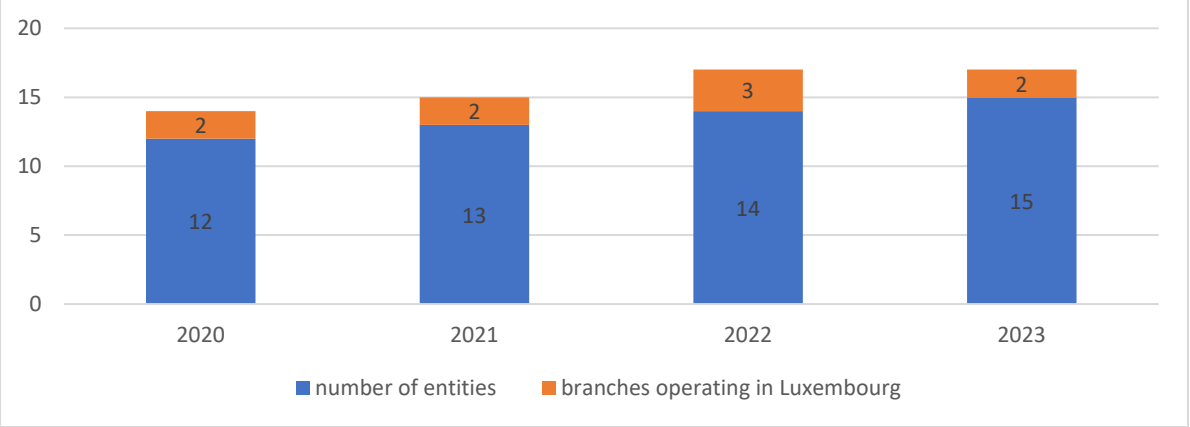
#### 6.1.3.1. *Payment institutions*

**AT A GLANCE**

The 2025 NRA assesses the inherent ML 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 (which was reassessed upwards to account for new data about foreign ownership of these entities) and international business.

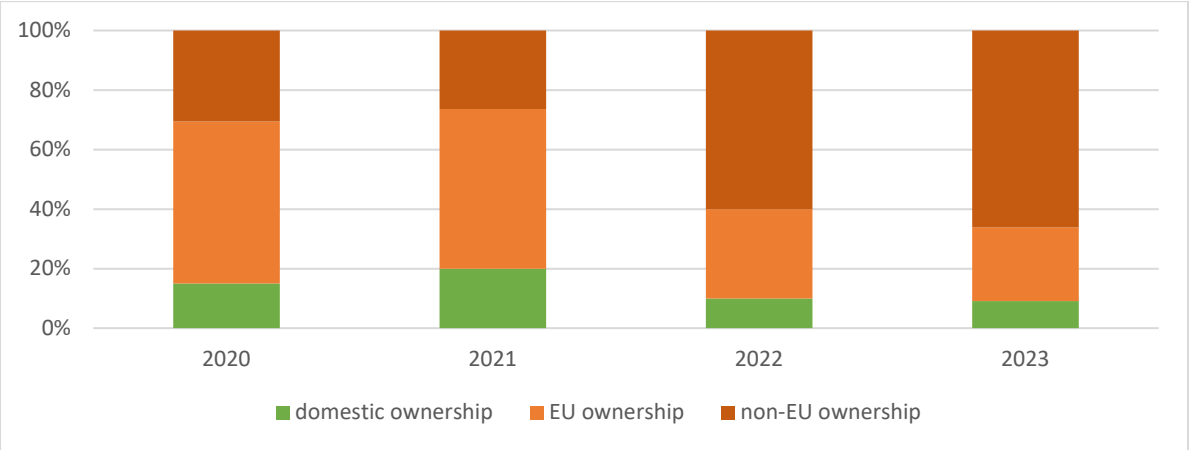
The number of PIs in Luxembourg slightly increased in comparison to 2020, with 15 entities in 2023, as shown in the figure below.

**Figure 16: Number of payment institutions and branches in Luxembourg, 2020 - 2023**




Following the increasing number of players in the market, concentration decreased through the observation period. In 2020, top-five entities generated about the totality of the market's revenues. In 2023, the subsector remains still concentrated, although at a lesser extent (87% of the market's revenue generated by top-five entities).

**Figure 17: Breakdown of ownership (domestic, EU-ownership and non-EU ownership), 2020 - 2023**




As depicted in the figure above, ownership structure of the Luxembourg sub-sector has evolved and the share of non-EU owners has increased, contributing to the ML risk exposure.

As noted by the European Banking Authority (EBA), ML risks linked to products and services depend on the individual institutions' business models. Nonetheless, products allowing anonymity through new technologies, the use of innovative products, the high speed of transactions, the use of cash and the one-off type transactions without an associated payment account are presumed to amplify risk[212]. With regard to the payment services, these services may be used to layer and withdraw illicit funds from one's accounts (i.e. deposits on accounts and use of these accounts), especially if they allow the deposit and withdrawal of cash). They may also be abused by money mules[213].

[212] EBA, *Report on ML/TF risks associated with payment institutions 2023*, link.

[213] 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.

In Luxembourg, most PIs offer online payment services. Luxembourg's sub-sector risks related to cash-based services (i.e. allowing the withdrawal of cash from an ATM) was assessed to be very limited, representing on average 0,09% of the total outflows processed by these PIs. Nonetheless, the risks outlined in relation to the high speed of transactions, one-off transactions and the general risks that apply in an online environment (cf. CEF) are also valid for this particular sub-sector.

The number of clients served by Luxembourg PIs reached its peak in 2022 with 21 million clients. In 2023, the number of clients has decreased by 37% (to 13,2 million) due to the transfer of a significant number of clients of one PI to another entity of the group outside of Luxembourg. This remaining important volume, combined with the still significant number and value of transactions processed drives ML risks. However, this is partially compensated by the low proportion of high-risk clients in the sub-sector. Indeed, on average, only 0,7% of clients were considered as high risk by those entities during the observation period.

Most of PI's clients were natural persons, although their share has decreased throughout the observation period (96% in 2020 and 2021 in comparison to 91,3% in 2023). According to the EBA, it is presumed that PIs' focusing on cross-border outlooks present a higher ML risk than those focusing on a local market. Overall, it can be said that the clientele of Luxembourg's PIs was mainly foreign. The share of clientele from EU countries is volatile over the observation period, ranging from 54% to 96%.

Considering that consolidated flows followed a similar trend, risks with regard to international business was considered to be significant.

**Table 14: Consolidated flows (EU and non-EU countries), indicative data, 2020 - 2023**

| | Consolidated flows with EU countries | Consolidated flows with non-EU countries |
|---|---|---|
| **2020** | 91% | 9% |
| **2021** | 75% | 25% |
| **2022** | 71,4% | 28,6% |
| **2023** | 83% | 17% |

Nonetheless, it should be noted that exposure towards high-risk geographies remains limited (on average 1,35% of consolidated flows[214]), decreasing the overall ML risk score of PIs.

Almost all Luxembourg PIs onboarded their clients via non-face-to-face channels in 2023. This is assessed to bear significant ML risks.

#### *6.1.3.2. E-money institutions*

**AT A GLANCE**

SNRA

The 2022 SNRA assesses the ML risks related to the e-money sector as high. The main contributing factors are the distribution channels (use of intermediaries). Other risk factors mentioned in the 2022 SNRA are the sector's extensive reliance on non-face-to-face identification processes

[214] As per CSSF internal rating list.

(increasing risks of computer fraud and use of false documents), the anonymity of the customer for some of the products as well as the ease and speed of e-money transactions.

NRA

The 2025 NRA assesses the inherent risk level as "High". EMIs share the same key risk drivers as PIs: volume of transactions performed, products and activities and distribution channels, followed by size, ownership/legal structure, size and international business.

In Luxembourg, the sub-sector was similar in size and activities to the PIs sub-sector, and thus shares similar inherent vulnerability to ML risk. As evidenced in the table below, EMIs experienced significant growth over the last couple of years.

**Table 15: Comparison of statistics related to EMIs, 2018 and 2023 data**

| | 2018 figures (2020 NRA) | 2023 figures (2025 NRA) | Variation (in %) |
|---|---|---|---|
| **Number of EMIs operating in Luxembourg** | 6 | 10 | +66% |
| **Balance sheet total (in EUR billion)** | 1,8 | 7 | +289% |
| **Number of inflow transactions (in billion)** | 1,3 | 2,5 | +92% |
| **Number of outflow transactions (in billion)** | 0,05 | 0,17 | +240% |
| **Total value of inflow transactions (in EUR billion)** | 38,4 | 107 | +179% |
| **Total value of outflow transactions (in EUR billion)** | 27,4 | 78,7 | +187% |

In comparison to the total volume and value of transactions within the EU, Luxembourg's EMI sub-sector accounts for a decreasing, but a significant share of these transactions[215;216].

However, exposure to ML risks were partially reduced by the very high concentration rate within the Luxembourg sub-sector. Throughout the observation period, top-five entities generated on average 99% of the market's revenue.

The Luxembourg EMI sub-sector served an increasing number of customers throughout the observation period (25 million in 2020, 38,3 million in 2021, 47 million in 2022 and 82,8 million in 2023). It should be noted that the arrival of new players on the market partly explains this surge. With this in mind, ML risks related to the criteria size and client (volume) are assessed to be respectively high and very high.

Overall, both the 2022 SNRA and the EBA note that prepaid cards and, especially those that may be loaded by cash, are particularly vulnerable to ML. The products' inherent features, such as the ease and speed of transactions contribute to these risks[217]. In this context, it should be noted that

[215] Eurostat, *Total number of e-money payment transactions all, sent – from: euro area (changing composition), Euro area (Member States and Institutions of the Euro Area) changing composition, Annual,* retrieved January 14 2025, link and Eurostat, *Total number of e-money payment transactions all, sent – from: Luxembourg, Luxembourg, Annual,* link retrieved on 14 January 2025.

[216] Eurostat, Total value of e-money payment transactions all, sent - from: euro area (changing composition), link and Eurostat, Total value of e-money payment transactions all, sent - from: Luxembourg, link retrieved on 14 January 2025.

[217] 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 and EBA, *Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector*, 2023, link.

Luxembourg EMIs offered e-money accounts and wallets. Cards linked to e-money accounts allowed cash withdrawals. Those withdrawals amounted to EUR 430 million (i.e. 0,54% of the total outflows processed by EMI) in 2023. None of the Luxembourg EMIs offered prepaid cards, limiting exposure to ML risks to some extent.

Between 2020 and 2023, most clients resided in the EU although their share decreased continuously with 90% in 2020, 83% in 2021, 81,5% in 2022 and 76,4% in 2023. This increases ML risks and the proportion of clients residing in high-risk countries averaged 5% between 2020 and 2023[218].

As already noted previously, the sub-sector counts an important number of customers, with most being natural persons (about 90%). The number of clients being marked as high-risk by the entities is in line with the other banking sub-sectors providing payment and basic account services, namely around 1%. Client risk is, therefore, considered to be moderate.

Similar to PIs, EMIs operated mainly online. Consequently, channels employed were 100% non-face-to-face, increasing ML risks.

#### *6.1.3.3. Agents and e-money distributors acting on behalf of PIs/EMIs established in other EU Member States*

**AT A GLANCE**

Based on the 2025 NRA, the inherent risk level of agents and e-money distributors acting on behalf of PIs/EMIs established in other EU Member States remains "Medium".

Key risk drivers for agents and e-money distributors acting on behalf of PIs/EMIs established in other EU Member States are products and activities followed by geography.

In 2023, the market size for agents and e-money distributors remained limited, with 19 agents working on behalf of six PIs established in other EU Member States. Fragmentation 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.

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, there is often no possibility to assess the customer's behaviour and monitor its transactions.

As regards e-money distributors[219], the main funding payment method was payment cards (94%). The remaining 6% were cash-based (gift cards)[220]. Globally, e-money distributors are mainly distributing prepaid cards and vouchers that can be used to buy goods and services from a wide range of merchants. These prepaid cards and vouchers might offer a degree of anonymity when they are used as the buyer of the goods and services is not identified by the merchants. In addition, customers can buy the prepaid cards and vouchers which in turn can be used by another person to whom the

[218] As per CSSF internal rating list.

[219] It has to be noted that the e-money distributor is no longer active since beginning of 2022.

[220] CSSF, *Agents/e-money distributors Guidance for the prevention of money laundering and terrorism financing*, 2022, link.

customers have given the prepaid card or voucher as gift. This makes it difficult to obtain information from the parties involved[221].

Considering the above, the ML risks related to the criterion "products and activities" for agents and EMI distributors are assessed to be very high.

Most (99,9%) of their customers were natural persons, with 8% being marked as high-risk (based on entities' internal risk assessment in 2021). Around a quarter of total consolidated flows in 2021 were within high-risk countries (as per CSSF internal rating) and 64% of consolidated flows were with EU countries[222]. In comparison to the other sectors, the share of high-risk clients and flows with third countries were considered to be high.

Both agents and distributors typically meet their clients face-to-face[223]. This had a positive impact on the risk scoring allocated to distribution channels.

### *6.1.4. Virtual assets service providers*

**AT A GLANCE**

At a product level (SNRA, NRA)

The 2022 SNRA assesses the risks associated with crypto assets and virtual currencies as very high, due to their characteristics (internet-based, cross-border, …).

In the NRA, risks related to the products and services offered by VASPs are assessed under the dimension "products/activities". For the case of Luxembourg VASPs, these products and activities are assessed as having high ML risks.

At a sub-sector level (NRA)

In Luxembourg, the 2025 NRA assesses the inherent risk of VASPs as "High", with key risk drivers being volume of clients/transactions and distribution channels, followed by size, ownership/legal structure, products/activities and the international nature of the business.

VASPs were identified and assessed as an emerging risk in the 2020 NRA. They were analysed in a dedicated VRA, including a detailed assessment of ML inherent risks emerging from virtual assets (VAs) and VASP activities as well as a description of the mitigating factors. The 2025 NRA integrates VASPs in the NRA taxonomy, updates and completes the assessment of VASPs following the NRA methodology.

The number of entities registered with the CSSF as VASPs has increased steadily since 2021, although total number remains still relatively low. Whereas the sub-sector counted 6 entities in 2021, it was composed of 11 entities in 2023:

- two were already operating under the licence of a PI;
- one under the licence of an EMI;

[221] CSSF, *Agents/e-money distributors Guidance for the prevention of money laundering and terrorism financing*, 2022, link.
[222] CSSF data.
[223] CSSF data related to 2021.

- two under the licence of a bank; and
- six were exclusively providing VA services in Luxembourg.

Whereas the sub-sector was entirely controlled by foreign entities/persons in 2021 and 2022, foreign ownership decreased in 2023 and amounted to 88% (with the majority remaining under non-EU control).

With respect to products and services offered by Luxembourg VASP:

- Most (10 out of 11) entities registered with the CSSF offered safekeeping of VAs and/or administration of instruments enabling control on VAs. These services were assessed to bear "medium" risk in the VASP dedicated risk assessment.
- The transfer of VAs was also offered by 9 out of the 11 entities. This service is known to bear "high" risk as VAs inherent product features (pseudo-anonymity, and speed of transactions) make them attractive for ML abuse.

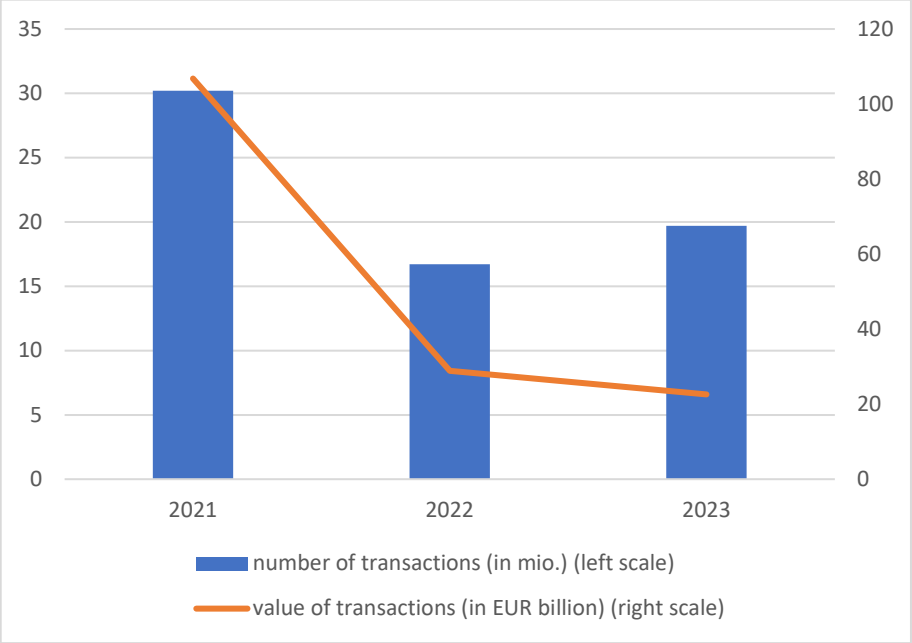
The 2022 SNRA concludes that criminal organisations use virtual currencies and VAs to transfer value, to purchase goods anonymously or to access "clean cash" (i.e. paying in and out). In this respect, the 2022 SNRA highlights that corruption and bribery, child sexual exploitation, investment fraud, and counterfeit goods are related predicate offences that may be encountered with regard to the transfer of virtual currencies and VAs.

The number of clients has fluctuated heavily during the observation period. Whereas the number of clients surged by 56% between 2021 and 2022, it fell by 63% between 2022 and 2023. This significant decrease is linked on one side to the change of the business model of one entity for the services offered to the UK market to comply with UK requirements, and on the other side to the difficult market conditions observed in 2022 and 2023 (crypto-winter).

Whereas in 2021 and 2022 most deposits were from EU countries (77%) with the remainder coming from the UK, the situation has changed in 2023 with almost all deposits being from the EU (92%). With respect to transfers, the shift towards a more European market may also be observed with around 65% being from EU countries in 2021 and 2022, in comparison to 84% in 2023. Here, Switzerland was the most encountered non-EU country. Overall, and considering the sub-sector's fluctuations with regard to its international outlook, inherent ML risks are considered to be significant.

The volume and value of transactions of the exchange of VA against fiat currencies and the exchange of VA against another type of VA processed by the Luxembourg sector decreased heavily between 2021 and 2023, as depicted in the figure below. This strong decrease is linked to the change of business model of one entity mentioned above as well as to the market situation. Nonetheless, analysed indicators (i.e. value and number) remained high.

**Figure 18: Number and value of transactions of the exchange of VA against fiat currencies and the exchange of VA against another type of VA, 2021 – 2023**




Overall, Luxembourg registered VASPs generated 30,2 million of transactions of exchange of VA against fiat currencies and the exchange of VA against another type of VA worth EUR 106,8 billion in 2021. The total number of transactions and associated value fell sharply in 2022 (16,7 million of transactions worth EUR 28,9 billion) and 2023 (19,7 million of transactions worth EUR 22,6 billion). A similar picture could be drawn for the volume and associated value of transfers of VAs. However, safekeeping services of VAs (activity concentrated on one VASPs which is also a PI) increased through the observation period from EUR 2,6 billion equivalent in 2021 to 5,9 billion equivalent in 2023. This said, the VASP sector processed a still significant number of transactions likely to contribute to the exposure to ML risk.

Almost all clients (99%) were natural persons, and the number of PEPs remained very limited, decreasing exposure to ML risk.

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

### *6.1.5. Specialised PFSs*

**AT A GLANCE**

The inherent ML risk level of Specialised PFSs providing corporate services remains “High”, whereas the inherent ML risk level of professional depositaries remains “Medium”.

The specialised PFSs sub-sector can include various licenses, each offering different services. These licenses include registrar agents, corporate domiciliation agents, professionals providing company incorporation and management services, and family offices.

#### 6.1.5.1. *Specialised PFSs providing corporate services*

**AT A GLANCE**

The inherent ML risk level of Specialised PFSs providing corporate services remains "High". Overall key risk drivers continue to be fragmentation/complexity, international nature of business followed by products/activities and client risk.

Luxembourg counted 85 specialised PFSs (out of a total of 100 entities) providing corporate services with over 6 400 employees as of December 2023, with balance sheet assets of EUR 1,02 billion and profits reaching EUR 90 million. The sector remained quite fragmentated with top-five entities accounting for 40% of the market's revenues in 2023.

Vulnerabilities stemming from foreign ownership are assessed to be moderate, as 55% of specialised PFSs providing corporate services were under Luxembourg ownership, 19% under EU ownership (excluding Luxembourg) and 26% under non-EU ownership.

In Luxembourg, the ML risk remains driven by the fact that these PFSs offer TCSP activities (cf. section 6.6.1). They are often involved in the establishment and administration of legal persons and arrangements, playing a key role as gatekeepers of the financial sector.

Specialised PFSs providing corporate services' clientele were almost entirely made up of legal persons (99%). More than half (61%) of the client companies' BOs resided in non-EU countries and 1,46% resided in a high-risk country[224]. Exposure to a non-EU clientele remains a significant vulnerability to ML for this sub-sector.

With the overall number of clients of specialised PFS providing corporate services being rather limited (with over 30 000 client companies in 2023 and 20 000 in 2020), exposure to ML risks is considered to be moderate. Nevertheless, specialised PFSs providing corporate services have identified one in five client companies as high risk and around 4% of client relationships involve PEPs (e.g. a PEP being the BO, legal representative, etc.). Although this share has decreased over the observation period, this figure remains high, driving ML client risk.

Channels used by the sub-sector pose moderate ML risks. Most players have direct relationships with clients and intermediaries are business providers (accountants, ...) including the group to which the PFS belongs.

#### 6.1.5.2. *Professional depositaries*

**AT A GLANCE**

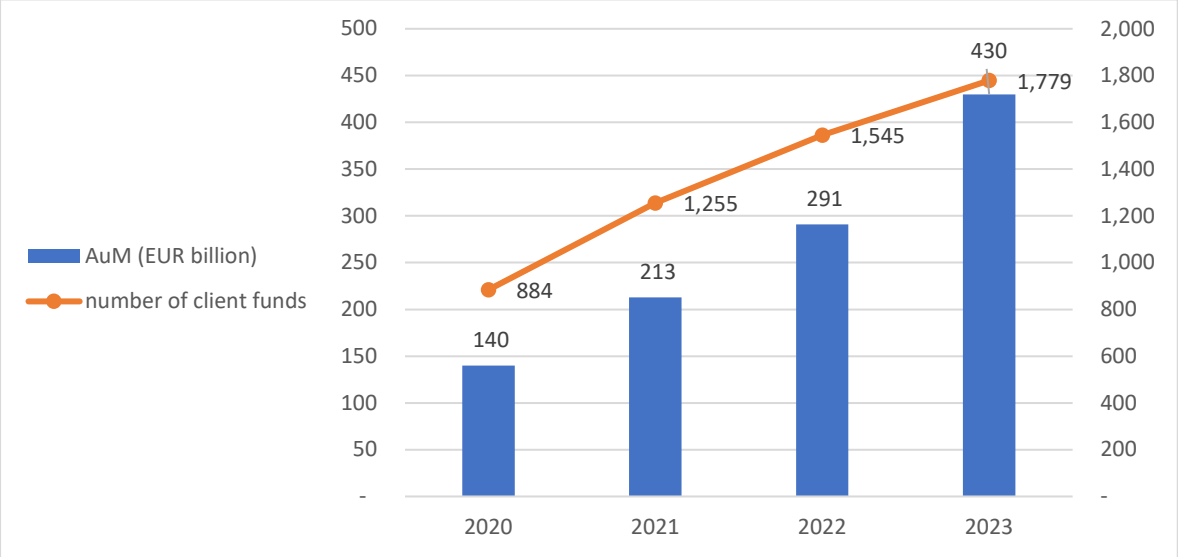
The inherent risk level of professional depositaries is assessed as "Medium". Key risk drivers are the sub-sector's size and client risk.

The 2020 NRA identified that the main vulnerabilities of the specialised PFSs sector stem from the large size of the professional depositaries sub-sector. In this regard, it is interesting to note that the number of professional depositaries of assets other than financial assets has remained stable since

[224] As per CSSF internal rating list.

the 2020 NRA. Nevertheless, the sub-sector's AuM and number of client funds experienced a significant increase, as evidenced in the figure below.

**Figure 19: Increase of AuM and number of client funds of professional depositaries of assets other than financial instruments[225]**




Luxembourg counted 16 professional depositaries of assets other than financial assets and one professional depositary of financial assets with 2 567 employees in 2023.

Ownership complexity was assessed to bear moderate risk, as 53% was under Luxembourg ownership and 47% under non-EU ownership (Jersey, UK and USA).

In 2023 (2020), 98% (97%) of professional depositaries' clients were Luxembourg funds. The share of PEPs served in this sub-sector was relatively high, with more than 2% of the client relationship involving PEPs (e.g. as BO, legal representative). In addition, client funds included illiquid assets categorised as high-risk.

Risks posed by channels were assessed to be moderate as a high number of investment funds are set up/initiated by an entity belonging to the same group as the depositary.

### *6.1.6. Support PFSs and other specialised PFSs*

**AT A GLANCE**

Support PFSs and other specialised PFSs continue to have a very low exposure to ML activities, due to the limited financial services client interaction and the low-risk nature of their activities (that is, IT related and other support services).

#### *6.1.6.1. Support PFSs*

Support PFSs include client communication agents (article 29-1 of the LSF), administrative agents of the financial sector (article 29-2 of the LSF), IT system communication network operators in the

[225] CSSF data.

financial sector (article 29-3 of the LSF), dematerialisation service providers (article 29-5 of the LSF) and e-archiving service providers (article 29-6 of the LSF).

As of 2023, there were 60 (vs. 71 in 2020) support professional service providers operating in Luxembourg, employing 7 716 people (vs. 8 987 in 2020). Of these 60 entities, 12 were client communication agents and administrative agents, and 30 were IT system operators. Two of these 30 entities had additional agreements for dematerialisation or e-archiving service provision. A few professionals hold licenses to offer activities both as Specialised PFS and Support PFS. In such cases, they are taken into account under both categories.

#### *6.1.6.2. Other specialised PFSs*

Some specialised professional service providers, which have been included under this section, are less exposed to ML risks compared to the wider specialised PFS sector due to the nature of the services provided. In 2023, four professionals perform lending operations (article 28-4 of the LSF) and two debt-recovery services providers (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 ML purposes in Luxembourg.

### *6.1.7. Market operators*

**AT A GLANCE**

Market operators' inherent risk level remains "Low".

Exposure to ML risks is limited due to the presence of only one market operator – the Luxembourg Stock Exchange (LSE). A certain inherent risk exists due to the significant volume of issuance activities (EUR 1 218 billion of debt issued via instruments admitted to trading on the LSE in 2023) and the international nature of the transactions executed on the LSE markets. However, the vulnerabilities associated with LSE clients and transactions remain low because the small number of members to which the LSE is open are all investment firms or banks subject to AML/CFT obligations and due to the low transactions volume (trading volume of EUR 135,43 million and equity trading volume of EUR 38 million in 2023).

## 6.2. CAA supervised sectors

The inherent risk levels for the sectors falling within the AML/CFT supervision of the CAA are shown in the table below.

**Table 16: Inherent ML risk of the insurance sector - overview by sub-sectors (CAA supervised sectors)**

| Sector | Sub-sectors | 2025 NRA: Inherent risk |
|---|---|---|
| Insurance | Life insurance | High |
| | Non-life insurance | Low |
| | Reinsurance | Low |
| | Intermediaries | Medium |
| | Professionals of the insurance sector (PSAs) | Low |
| | CAA-supervised pension funds | Very Low |

Globally, the insurance sector is typically regarded as less vulnerable with regards to ML risks than other financial products or other sectors[226]. Insurance products are less flexible than other financial products, such as loans or payment services, limiting their attractiveness for ML activities by criminals. Furthermore, insurance products are complex for ordinary criminals, requiring some specific knowledge. In addition, pay-outs from insurance undertakings are unpredictable and/or risky as they are dependent on the incident that has been insured actually taking place (e.g. death or tail events).

Despite this, certain features of insurance products can add to sectorial inherent risks for the insurance sector and make them particularly vulnerable to ML, namely, when they have flexibility of payment and investment, ease of access to accumulated funds, negotiability (i.e. can be used as collateral), involve early termination, changes in beneficiaries and payment forms.

### *6.2.1. Life insurance*

**AT A GLANCE**

SNRA

Overall, the SNRA assesses the ML risks related to the life insurance sub-sector as "moderately significant" (Medium) with the ML risk mainly stemming from the investment related components, such as paying a high one-off premium or capital accumulation. In addition, life policies could be redeemed early to generate lump sums and the proceeds can be transferred to beneficiaries with whom life insurance undertakings often do not have client relationships. Nonetheless, ML abuse in this sub-sector is generally the result of sophisticated schemes, requiring a considering level of expertise and planning.

NRA

[226] FATF, Guidance for a risk-based approach for the life insurance sector, 2018, link.

The 2025 NRA assesses the ML risks related to the life insurance as "High" (unchanged to 2020 NRA), with key risk drivers stemming from sub-sector size and volume of clients. Nature of products/activities (in line with the EBA opinion[227] and the SNRA), orientation towards foreign residents and the relative share of high-risk clients and distribution channels (see also the EBA opinion) are other risk drivers still relevant.

The life insurance sub-sector remained large between 2020 and 2023. As of end 2023, this sub-sector showed a balance sheet total of EUR 234 billion, EUR 234 billion in technical provisions, EUR 21 billion in premiums and 3 102 employees across 36 undertakings falling within the AML/CFT scope[228]. Slightly more than half of gross written premiums were generated by five entities[229].

Overall, the EBA noted in its opinion that tax-related crime is still considered an important threat to the sub-sector. A case study related to tax fraud linked to life insurance policies is provided below.

**Case study 13: Tax fraud case[230]**

A case was initiated based on an MLA request from country A concerning two nationals from country A (a couple) residing in country B. The request sought to search and seize funds in Luxembourg bank accounts identified as belonging to them. The alleged offenses were aggravated tax fraud and ML. Besides that, the couple was also reported to the CRF. Information was provided about two life insurance policies subscribed by the suspects with an insurance company based in Luxembourg. The CRF's analysis revealed that several additional payments had been made to these policies since their subscription amounting to approximately EUR 3 million. It was further identified that the initial payments were made through an account in country A held by the husband.

According to available information, the funds used for the life insurance policies came from the sale of a company based in country A, run by the husband's family, as well as from his professional income. The CRF could not dismiss the suspicion that the funds invested in the insurance policies might have originated from aggravated tax fraud and consequently issued a freezing order.

The CRF's counterparts, as well as the State Prosecutor's Office, were informed of the existence of additional assets in Luxembourg which were not covered by the initial MLA request.

An additional MLA request was received by the General State Prosecutor's Office and the insurance policies were subsequently seized in Luxembourg.

Furthermore, the EBA assessed that the types of products and operations representing the main ML risks are products with a short maturity period, like insurance-based investment products with a minimum holding period of 5 years, and those with the possibility of early termination of the policy. Other products with higher ML risks are investments associated with large life insurance policies. The most exposed insurance contracts, both single premium and regular premium, are unit-linked

[227] EBA, *Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector*, 2023, link.

[228] CAA data 2023. The numbers also include six Luxembourg branches of foreign FIs.

[229] CAA data 2023.

[230] Case study provided by the CRF.

products with a high financial component and a low insurance component where the repayment of capital and interest is basically agreed.

In 2023, the Luxembourg life insurance sub-sector continued to be oriented towards foreign residents, increasing the sector's exposure to ML activities and high-risk clients. The majority (94%) of premiums were linked to foreign countries, among which 9% from non-EEA countries (mostly the UK and Switzerland). About 0,95% of clients were PEPs.

The average holding period of insurance-based investment products ranges between 8 to 12 years depending on the characteristics of the products, its clients and geographical area. As at the end of 2023, unit linked products represented around 79% of the total amount of the technical provisions of the life insurance sub-sector.

Other ML risk factors included the high volume of transactions and the usage of intermediary distribution channels. In 2023, over 295 000 new contracts were sold. With regard to distribution channels, 94% (in terms of premiums) were sold through intermediaries[231], which can increase exposure to ML risk.

**Case study 14: Source of funds (non-Luxembourg case)[232]**

A husband and wife took out a life insurance policy each in their own name with annual premiums. In the event of the death of one of the spouses, the other spouse would become the beneficiary of the insurance. The holder of the account through which the premiums had been paid was found not to be the policyholders but a company abroad of which they were directors. However, this was a life insurance policy taken out privately by the couple and not by the company. Investigation revealed that the scenario set up had been intended to conceal the illicit origin of the funds which originated from serious and organised tax fraud for which the couple involved was known.

### *6.2.2. Non-life insurance*

**AT A GLANCE**

SNRA

The 2022 SNRA notes that the non-life insurance sector is quite unattractive for ML purposes due to the high level of planning and expertise required.

NRA

The 2025 NRA assesses the sub-sector inherent risk level as "Low".

In Luxembourg, the non-life insurance sub-sector is smaller than the life insurance sub-sector. As of 2023, it had EUR 60 billion in total balance sheet, EUR 40 billion in technical provisions, EUR 19 billion in premiums and 9 511 employees across 43 undertakings. With around 64% of written gross premiums generated by five entities, the sector was more concentrated than the life-insurance sub-sector[233]. Around 92% of premiums were linked to foreign countries among which 67% were linked to

[231] CAA data 2023.

[232] IAIS, Application Paper on Combating Money Laundering and Terrorist Financing, November 2021, link.

[233] CAA data 2023.

EU countries. Premiums linked to non-EU countries mainly concerned the UK, the USA and Switzerland.

The low ML risk is explained by the low-risk nature of products, as products offered are not inherently risky. Indeed, they pay out against a pre-defined event, have no surrender value, no investment elements and the premiums are generally of lower value. Moreover, only 18 undertakings offered classes 14 (credit) and 15 (suretyship) and thus fell within the AML/CFT scope[234]. Out of those 18 undertakings, 7 were EU owned and the remaining 11 were non-EU owned. They generated EUR 1 237 million of gross premium in 2023.

### *6.2.3. Reinsurance*

**AT A GLANCE**

The 2025 NRA assesses the sub-sector's inherent risk level as "Low".

As of end 2023, the reinsurance sub-sector counted 51 traditional reinsurance undertakings and 144 reinsurance captives (i.e. 195 entities in total). This sub-sector was relatively concentrated with almost 71% of written gross premium generated by five entities.

The business of the reinsurance sub-sector remained highly international. Nearly 27% of accepted premiums were written through ceding companies located in the UK, 12% in France, 14% in Germany, 5% in Spain and 17% in other EEA countries, limiting business with riskier geographies.

Compared to the sub-sector of life insurance, ML risks are reduced by the low-risk nature of products as reinsurance is available by insurance undertakings acting as customers.

Moreover, less than 22% of the reinsurance sub-sector (i.e. 42 entities) fell within the AML/CFT scope as they reinsure credit and suretyship risks.

Among those 42 entities, most of them (37, i.e. 88%) were EU owned in 2023 and the remaining 5 had non-EU ownership.

### *6.2.4. Intermediaries*

**AT A GLANCE**

The 2025 NRA assesses the sub-sector's inherent risk level as "Medium".

The following risk drivers are relevant: sub-sector size, international nature of business and volume of clients/transactions. The sub-sector's inherent ML risk has been assessed "Medium" (compared to "High" in 2020 NRA) taking into account enhanced concentration of brokerage firms and the low number of PEP clients.

As of end 2023, the intermediaries sub-sector counted 90 brokerage firms, 119 brokers, 462 insurance sub-brokers and 258 insurance agencies. Ownership was mostly from the EU (85%, including 30% of

[234] CAA data 2023. The numbers also include two Luxembourg branches of foreign entities.

shareholders from Luxembourg) and the remaining 15% ownership were primarily from the UK and from Switzerland.

The high volume of transactions is a key vulnerability driver in this sub-sector. The new premium flows in 2023 amounted to EUR 1,95 billion for life and EUR 1,1 billion for non-life. More than half (60%) of the life insurance premium flows were distributed by five intermediaries. Among these five intermediaries, three are also banks under double supervision with the CSSF, one is a subsidiary of a bank also supervised by the CSSF and one is a "traditional" brokerage firm. The ML risk is also driven by the high international nature of the business. As such, brokers had mainly international clients (93% of premiums from foreign countries for life and 85% for non-life) mostly focused on the EEA market (non-EEA represents 9% of life and 17% of non-life premia). However, there was no premium written with a life insurance undertaking situated in a high-risk geography. Also, 92% of premia were written with Luxembourg-based life insurance undertakings. The share of new contracts with PEPs as clients only totaled 0,12% in 2023.

### *6.2.5. Professionals of the insurance sector (PSAs)*

**AT A GLANCE**

The 2025 NRA assesses the sub-sector inherent risk level as "Low".

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 ML risk.

As of end 2023, Luxembourg counted 26 PSAs, out of which 13 were falling under AML/CFT scope[235]. The sub-sector was relatively concentrated with 87% 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).

### *6.2.6. CAA supervised pension funds*

**AT A GLANCE**

The 2025 NRA assesses the sub-sector's inherent risk level as "Very low".

Luxembourg counted three pension funds supervised by the CAA with EUR 661 million in balance sheet total. The total number of affiliates amounted to 10 088 in 2023. The ML risk is limited due to the very small sub-sector size, the low fragmentation and the low-risk products offered by these pension funds.

[235] CAA data 2023.

## 6.3. AED supervised sectors

The AED supervised sectors are presented together in a dedicated section and the level of inherent risk is shown in the table below.

**Table 17: Inherent ML risk by sub-sectors (AED supervised sectors)**

| Sector | Sub-sectors | 2025 NRA: Inherent risk |
|---|---|---|
| Real estate agents and developers | Real estate agents *(agents immobiliers)* | High |
| | Real estate developers *(promoteurs immobiliers)* | High |
| Freeport operators | | Medium |
| Dealers in goods | Precious metals/jewellers/clocks | Medium |
| | Car dealers | High |
| | Art/Antiques | Medium |
| | Luxury goods (e.g. *"maroquinerie")* | Medium |
| Gambling service providers | Casino | Medium |
| | National lottery | Low |
| Legal and accounting professions supervised by the AED | Accountants | High |
| | Professional directors and business centres | High |

### *6.3.1. Real estate agents and developers*

**AT A GLANCE**

At the product level (SNRA)

The 2022 SNRA analysed risks associated to investments in the real estate sector and concludes that its ML risks are 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 is mostly used in combination with other professionals, such as TCSPs or legal advice.

At the sub-sector level (NRA)

The inherent risk associated with Luxembourg's real estate agents and developers is assessed as being "High" with key vulnerabilities stemming from the products and services offered by these professionals.

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 2023[236].

[236] STATEC, Gross value added by activity (NaceR2)(at current prices) (in millions EUR) 1995 – 2023, code L, link.

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. For instance, the split of deeds containing a tax credit clause ("*bëllegen Akt*") and a reselling clause are as follows:

**Table 18: Notarial deeds of sale and sales in future state of completion[237]**

| | Deeds including a tax credit clause ("*bëllegen Akt*") | Deeds including a reselling clause ("*clause de revente*") |
|---|---|---|
| **2020** | 8 181 | 1 335 |
| **2021** | 8 801 | 1 453 |
| **2022** | 6 970 | 1 135 |

**Insight Box 12: Tax credit clauses applying to real estate transactions**

***"Bëllegen Akt"* – tax credit on notarial instruments**

Natural persons who wish to acquire property for residential purposes may apply for a tax credit on notarial instruments. A tax credit can only be used once per buyer and the buyer has to occupy personally, as owner, the property acquired within a time limit of:

- two years from the date of the notarial deed of acquisition; or
- four years in the event of the acquisition of a building plot or a building under construction.

The buyer has to live in the property for at least two years. This tax credit is limited to EUR 30 000 per property buyer[238].

**Notarial deeds including a "*clause de revente*" in the case of real estate transactions**

The buyer of real estate may acquire the property with the intention/aim to resell it afterwards. In this case, (s)he may decide to add a "*clause de revente*" into the notarial deed of purchase. Although registration tax is higher with a "*clause de revente*" (i.e., 7,2% instead of 6%), the buyer of the property receives:

- a refund of 6% of the registration tax paid if the property has been resold within two years; and
- a refund of 4,8% of the registration tax paid in case the property has been resold within four years.

It should be noted that where the property was sold after four years, there is no refund of the registration tax.

In a similar vein, most persons registered with the notarial real estate deeds are natural persons:

[237] Chambre des Députés, *Réponse à la question parlementaire n°7781*, 2023, link.

[238] It should be noted that the tax credit increased from EUR 20 000 to EUR 30 000 per property buyer pursuant to the Law of 16 May 2023. For notarial deeds signed in 2024, the tax credit increased from EUR 30 000 per property to EUR 40 000 pursuant to the Law of 22 May 2024.

**Table 19: Breakdown between natural and legal persons regarding notarized deeds of sales and sales in future state of completion[239]**

| | Natural persons | Legal persons |
|---|---|---|
| **2020** | 11 262 | 1 542 |
| **2021** | 11 328 | 1 694 |
| **2022** | 9 167 | 1 403 |

#### *6.3.1.1. Real estate agents*

Luxembourg counted 2 528 real estate agents (REA) in 2023[240]. Overall, the sub-sector remains fragmented with 50% of REA generating a turnover less than EUR 120 000 during the observation period, 33% generating a turnover between EUR 120 000 and EUR 620 000 and about 17% generating a turnover exceeding EUR 620 000. Indeed, top-five real estate agents generated 24% of total market turnover in 2023.

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

#### *6.3.1.2. Real estate developers*

The number of real estate developers (REDs) has risen by around 9,5% in 2023 (1 799 REDs) in comparison to 2020 (1 496). In 2022 and 2023, approximately 42% of REDs had a turnover below EUR 120 000, 25% between EUR 120 000 and EUR 620 000 and 34% over EUR 620 000. Top-five REDs accounted for 16% of the market's turnover in 2023. Although the REDs' sub-sector is relatively less concentrated than the REAs sub-sector, it still remains fragmented.

### *6.3.2. Freeport operators*

**AT A GLANCE**

SNRA

The 2022 SNRA assesses the risk related to free-trade zones as "Very high" for ML purposes. The 2022 SNRA notes that Luxembourg has the only freeport within the EU (i.e., free trade zone specialising in the storage of high-value luxury goods) and that it is simultaneously the only one where information on the BO is available.

NRA

In the 2025 ML risks with regard to freeports are assessed as "Medium" inherent risk.

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

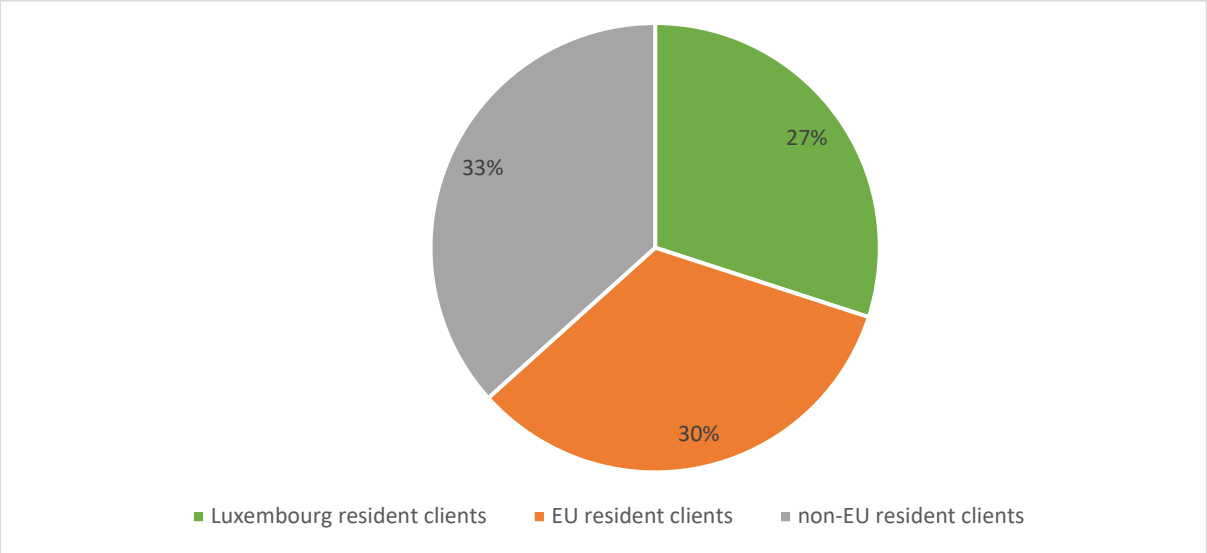
[239] Chambre des Députés, *Réponse à la question parlementaire n°7781*, 2023, link.
[240] AED data.

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.

In 2023, five licensed freeport operators rented space at the LHSH. One operator mainly worked for galleries and a local museum, one for art intermediaries, one was specialised in gold storage, one worked for banks (e.g. gold), and the last one was a local art museum.

ML risks are driven by the high-risk nature of activities (i.e. the storage of all kinds of high-value goods) although it should be noted that there were few transactions relating to the goods stored in the LHSH. In a similar vein, the number of clients remained stable throughout the observation period (between 90 and 100 clients). In 2023, the share of Luxembourg resident clients, EU resident clients (excluding Luxembourg) and non-EU resident clients was evenly distributed as shown in the pie chart below.

**Figure 20: Breakdown per country of residence of LHSH clients, 2023**




It should be noted that Luxembourg freeport 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[241]. Hence, the Luxembourg freeport may be less attractive for criminals, reducing exposure to ML risks.

### *6.3.3. Dealers in goods*

**AT A GLANCE**

SNRA

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

NRA

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

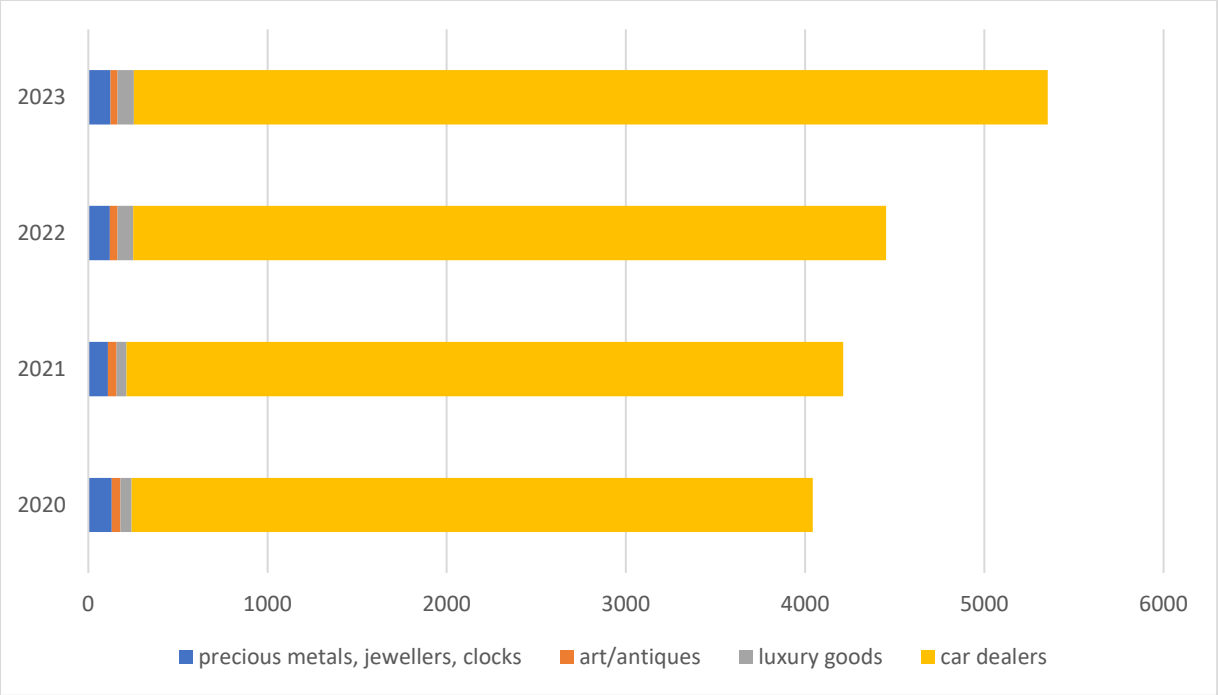
In the 2025 NRA, car dealers are assessed as having "High" ML risk due to the sub-sector's products and activities followed by the sub-sector's structure (i.e., size and fragmentation), international business and clients/transactions (volume and risk). ML risks related to the other dealers in goods (i.e., precious metals/jewellers/clocks, art/antiques and luxury goods) are assessed to be "Medium", with key risk driver stemming from these sub-sectors' products.

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"*).

Overall, Luxembourg counted 130 dealers in precious metals, jewellers and clocks, 136 art and antiques dealers and 650 car dealers in 2023.

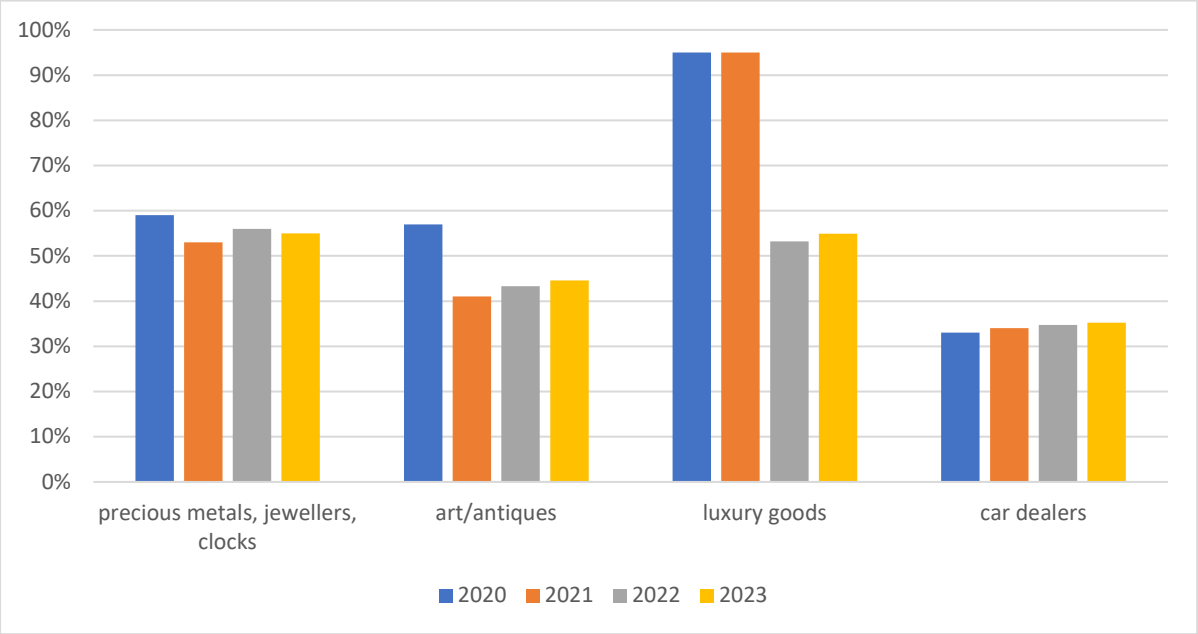
As evidenced in the figure below, the overall generated turnover has increased during the observation period and was predominantly (about 95%) generated by car dealers.

**Figure 21: Total turnover generated by dealers in goods, AED data (in EUR million)**




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) followed by dealers in precious metals, jewellers and clocks. In a similar vein, the sub-sector of car dealers presented the highest degree of concentration among the dealers in goods studied for the purpose of this report.

**Figure 22: Concentration rates: share of revenues generated by top-five entities (per category)[242]**




Although there is no limit on cash payments, the AED noted during its interactions with the private sector (through their supervisory activity and enforcement measures) 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 as well as car dealers.

**Insight Box 13: AED study on dealers in precious metals, jewellers and clocks' cash transactions**

The AED launched in 2023 a study on dealers in precious metals, jewellers and clocks' cash transactions for the years 2020 – 2022. This study is based on a review and analysis on all cash transactions performed by 29 professionals.

For these three years cash payments for these 29 professionals amounted to around EUR 40 million.

**Key findings of this study:**

- Cash payments have decreased by 8,8% between 2020 and 2022 (from around EUR 14 million in 2020 to EUR 12,78 million in 2022).
- 816 cash transactions were recorded between 2020 and 2022 with 68% (553 transactions) of them being related to transactions below EUR 10 000, thus falling out of the scope of the 2004 AML/CFT Law. The remaining 263 (32%) transactions were related to cash transactions exceeding EUR 10 000.
- Among these 263 transactions, most transactions were recorded in 2020. The number of cash transactions exceeding EUR 10 000 has continuously decreased since 2020 (113 in 2020, 96 in 2021 and 54 in 2022).

[242] AED data.

- The clientele's BO resided in 42,5% in Luxembourg. Residents from Luxembourg's neighbouring countries represented 44,8% of the BOs.
- In terms of value, cash transactions exceeding EUR 10 000 has decreased by 4,4% between 2020 and 2022 represented a total value of around EUR 3 million in 2020, EUR 2,4 million in 2021 and EUR 1,7 million in 2022.

### *6.3.4. Gambling service providers*

In Luxembourg, professionals providing gambling services are limited and mostly concentrated around the casino and the National Lottery. Between 2020 and 2023, there were no authorised domestic online gambling companies or sports betting firms and offline sports/horse betting is only offered by the National Lottery[243,244].

#### *6.3.4.1. Casinos*

**AT A GLANCE**

SNRA

The 2022 SNRA notes that the main ML risk posed by casinos is the risk of infiltration or ownership of organised crime groups. The document also notes that this risk is decreased in cases where regulations are in place imposing the transparency of beneficial ownership. Taking this into account, ML risks are assessed as "Medium".

NRA

The 2025 NRA assesses casino's inherent ML risk as "Medium".

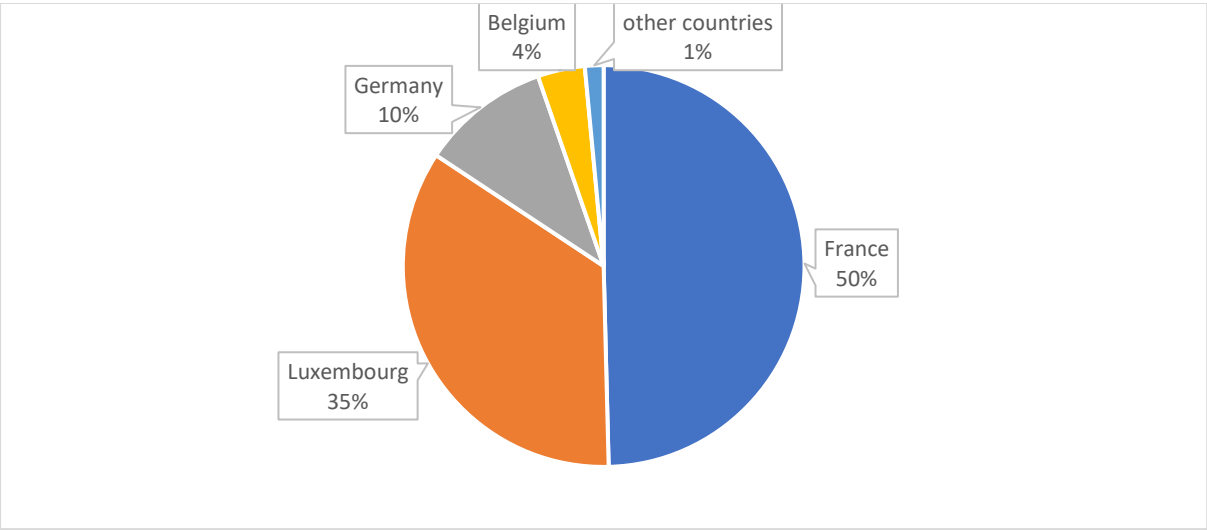
Luxembourg counts one privately owned casino with over 300 000 visitors in 2023. Many visitors enter the casino area in order to go to the casino's restaurant or to attend shows. The casino counted 148 employees in 2023 and generated revenues of EUR 56 million (of which EUR 50 million in gross gaming revenue (GGR)). With regard to products and activities, it should be noted that activities related to gambling are regulated. Slot machine were to be the most popular gambling activity.

The casino's client base was mostly a regional one, as shown in the next figure.

[243] PMU for horse betting, Oddset for sports betting.

[244] To note that the National Lottery has launched a sports betting site to contribute to combat illegal online gambling in September 2024. The vulnerabilities relating to this new offer will be analysed in the next NRA.

**Figure 23: GGR broken down by country of residence, 2023 figures**




It should be noted that all gambling activities required face-to-face interaction with casino staff. This made them less attractive for criminals for ML abuse.

#### *6.3.4.2. National Lottery*

**AT A GLANCE**

SNRA

The 2022 SNRA assessed the ML risks of lotteries as "moderate". Similar to casinos, there is a risk of infiltration or ownership by organised crime groups. Furthermore, a perpetrator may purchase a lottery ticket from the winner (possibly through collusion with the sales agent) and cash the price with the receipt. The 2022 SNRA also notes that this scenario is minimal in case of State-owned lotteries but increases at a retailer level.

NRA

The ML risks related to the National Lottery continue to be "Low".

As for the 2020 NRA, the ML risks of the National Lottery are very limited because of public ownership[245]. The National Lottery is operated by the *"Œuvre Nationale de Secours Grande-Duchesse Charlotte",* which is an *"établissement public"* (public entity) under the Law of 22 May 2009[246]. 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.

It should be noted that sales, GGR, points of sale and number of employees have increased since the 2020 NRA. The GGR amounted to EUR 76,8 million in 2023, EUR 63,6 million in 2022, EUR 54,7 million

[245] Note that private lottery operators are possible by Luxembourg law, but none are currently present.

[246] "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."*

in 2021 and EUR 50,5 million in 2020. Around 97% of GGR stemmed from lottery type games (e.g. instant games such as scratch cards) and the remaining 3% from sports/horse betting. Consequently, most of revenues stemmed from jackpot-driven games further reducing ML vulnerabilities linked to the product criterion.

The National Lottery counted 54 employees as of end 2023 (compared to 46 in 2020). As per 2020 NRA, revenues generated were split among a large customer base (mostly residents or residents of neighbouring countries) averaging 35 000 to 50 000 customers per week (which could go up to 80 000 – 90 000 customers during busy weeks).

The vast majority of customers are from Luxembourg or neighbouring countries, as sales are limited to the Luxembourg territory. 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.

Points of sale have increased at the same time of GGR. In 2023, the National Lottery counted more than 530 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[247].

**Insight Box 14: 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. Between 2020 and 2023, 20 lotteries were authorized at the national level. Overall, the amounts involved for these national ad hoc lotteries are likely to be limited: They each generated on average between EUR 40 000 and EUR 60 000, leading to an expected annual total of about EUR 260 000 amongst all of them. Furthermore, authorisations granted by the MoJ provide that 40% of the generated revenue is distributed as wins to the participants.

[247] National Lottery data.

### 6.3.5. *Legal and accounting professionals supervised by the AED*

**AT A GLANCE**

SNRA

The 2022 SNRA considers the ML risks related to legal and accounting professions as "High" due to the nature of services they may offer and their sector of expertise (create, register and/or manage LPAs, use of clients' accounts, prepare financial statements, provide assurance and guarantees, etc). These services may be misused by organised crime groups to disguise their identity, to commit predicate offences and to launder the proceeds of these crimes. These experts may be unwittingly involved in the ML but may also be complicit or willfully negligent in conducting their customer due diligence obligations.

NRA

The 2025 NRA assesses the ML risks of services offered by legal and accounting professionals for each category of professionals under the "products/activities" dimension. The inherent risk of legal and accounting professionals under AED supervision is assessed to be "High" with key vulnerabilities stemming in particular from fragmentation, ownership/legal structure and products and activities offered by those professionals.

#### 6.3.5.1. *Accountants*

The total number of accountants remained stable, averaging 649 accountants per year between 2020 and 2023. Whereas top-five players generated 20% of the market turnover in 2023 (i.e., EUR 270 million), top 100 players accounted for 74% 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.

#### 6.3.5.2. *Professional directors and business centres*

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)[248].

With respect to business centres, the AED identified over 65 business centres, with top-five players generating more than 40% of total turnover between 2020 and 2023. Overall, business centres supervised by the AED accounted for a total turnover of EUR 58 million (EUR 52 million) in 2023 (2020)[249].

[248] AED data.

[249] AED data.

## 6.4. Legal and accounting professions supervised by SRBs

**AT A GLANCE**

SNRA

The 2022 SNRA considers the ML risks related to legal and accounting professions as "High" due to the nature of services they may offer and their sector of expertise (create, registrate and/or manage legal persons and arrangements, use of clients' accounts, prepare financial statements, provide assurance and guarantees, etc). These services may be misused by organised crime groups to disguise their identity, to commit predicate offences and to launder the proceeds of these crimes. These experts may be unwittingly involved in the ML but may also be complicit or willfully negligent in conducting their customer due diligence obligations.

NRA

The 2025 NRA assesses the ML risks of services offered by legal and accounting professionals for each category of professionals falling under the "products/activities" dimension. As evidenced in the table below, the inherent risk levels for the sub-sectors falling within the AML/CFT supervision of the different SRBs:

**Table 20: Inherent ML risk of legal and accounting professions supervised by SRBs**

| Sector | Sub-sectors | 2025 NRA: Inherent risk |
|---|---|---|
| Legal and accounting professions supervised by SRBs | Lawyers | High |
| | Notaries | High |
| | Court bailiffs *(huissiers de justice)* | Medium |
| | Audit profession[250] | Medium |
| | Chartered professional accountants *(experts-comptables)* | High |

### *6.4.1. Lawyers*

**AT A GLANCE**

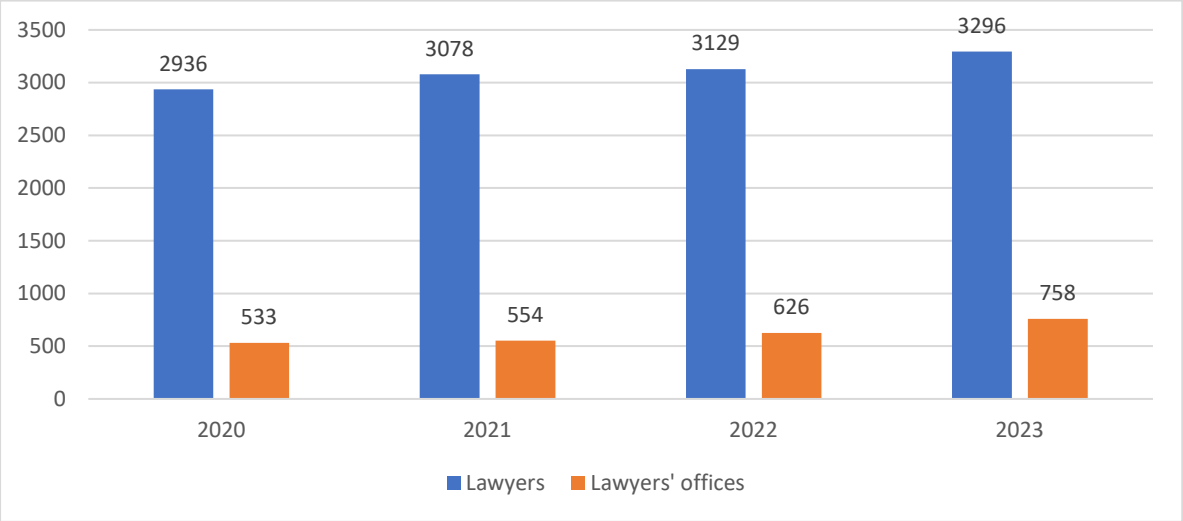
The sub-sector inherent risk level remains "High".

Size remains the main risk factor of this sub-sector. Although ML vulnerabilities associated to the sub-sector's products/activities have been reassessed downwards, they continue to be key risk drivers together with sub-sector's fragmentation, exposure to international business, including from risky countries, as well as the volume and risks related to the sector's clientele.

The number of lawyers registered with the *Barreau du Luxembourg* is large and has increased continuously since the 2020 NRA. In 2023, 3 296 lawyers (2 936 in 2020) spread across 758 lawyers offices (533 as of 2020) were registered with the OAL.

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

**Figure 24: Number lawyers and lawyers' offices registered with the OAL 2020 - 2023[251]**




About 38% of the lawyers were employed by the 10 largest law firms in 2023. It should be noted that 600 law firms counted less than 10 lawyers and, among those, 348 were represented by one lawyer[252]. Consequently, the important sector size and the fragmentation continue to be relevant for the studied purpose.

With respect to activities, the share of lawyers performing activities falling within the scope of the 2004 AML/CFT has also increased since 2020. Whereas 61% of OAL members indicated in 2020 to perform (from time to time) activities falling within the scope of the 2004 AML/CFT Law, 72% indicated to do so in 2023[253]. Nonetheless, most OAL lawyers focused predominantly on litigation and legal services and on legal mandates to a lesser extent. Those activities generally represent a lower risk for ML. 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.

As outlined in the 2020 NRA, TCSP activities are particularly vulnerable to ML abuse. In 2023, 13% of total lawyer's offices provided TCSP services in 2023. Among those, most of them offered domiciliation and directorship services.

Most of the profession's clientele resided in European countries[254] and North America. In both 2022 and 2023, around 10% of lawyer's offices had clients that had higher customer risk factors. Nonetheless, more than 80% of them noted that those clients represented less than 10% of their global volume of clients.

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.

[251] OAL data.

[252] OAL data.

[253] OAL data. 61,2% in 2020, 57% in 2021, 71% in 2022.

[254] Note that this term includes member states of the EU 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).

Among the lawyer offices falling within the scope of the 2004 AML/CFT Law, most of them declared generating between 1% and 10% of their turnover from the said activities.

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

### *6.4.2. Notaries*

**AT A GLANCE**

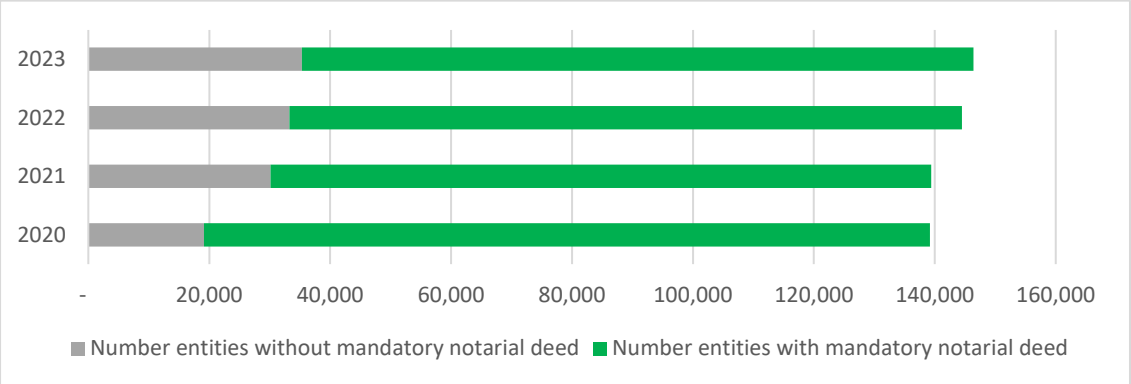
The ML inherent risk related to notaries is "High", with key risk drivers stemming from the size, products and activities, and international business.

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, nine new notaries were appointed between 2020 and 2023 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[255].

As touched on in the 2020 NRA and as further detailed in the VRA on ML/TF risks of legal persons and legal arrangements[256], 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).

The following graph represents the total number of entities registered with the RCS throughout the observation period of this NRA.

**Figure 25: Number of legal persons registered with the RCS, situation as of end 2020 - 2023[257]**




Although the share of entities created by notarial deed has slightly decreased during the observation period, two thirds of Luxembourg legal persons were registered by notarial deed.

[255] CdN data.

[256] MoJ, *ML/TF vertical risk assessment on legal persons and legal arrangements,* 2022, link.

[257] LBR data.

Compared to 2019, the number of total real estate mortgage transcriptions with the AED remained relatively stable at around 29 600 transcriptions[258,259]. 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.

Generally speaking, it is considered that corporate law activities tend to be more international than real estate or family law related activities. As highlighted in the 2020 NRA, 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. The initial ML risk of these professionals is considerably lower than those of offices showing predominant activities in areas which are more exposed to ML risks, as is the case, for example, in the context of international corporate activities, transactions implying larger cash flows etc. From 2020 to 2022 between five and seven notaries out of 36 indicated that corporate law accounts formed the largest part of their activities. In 2023, the number of notaries reporting that corporate law forms the largest part of their activities increased further. However, corporate law activities remained unchanged in terms of number of transactions performed. In fact, this shift is explained by the decrease in real estate activities. Nevertheless, there is a significant portion of international clientele in some notarial offices, especially in the ones that are specialized in business acts[260]. Hence, a conservative scoring for the "international business" criterion was applied.

### *6.4.3. Court bailiffs*

**AT A GLANCE**

The sub-sector inherent risk level remains "Medium".

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

Court bailiffs are subject to the 2004 AML/CFT Law when conducting public actions. The number of bailiffs active in this activity remains stable since 2018 at around 12. Most public actions are forced auctions following a legal decision or bankruptcy, whereas voluntary auctions by individuals or companies continue to be rather unusual. Given the limited number of auctions (74 in 2023, 58 in 2022, 84 in 2021, 55 in 2020) and the significant price range of goods sold during such events (for instance, from EUR 5 to EUR 63 000 in 2023 but from EUR 5 to EUR 1 million[261] in 2021), statistics related to average prices are subject to high volatility. Considering that the inherent nature of the court bailiff's profession (i.e. the recovery of funds), payments in cash are not unusual. However, they are capped at EUR 12 000.

ML exposure to geographical factors remains limited, in view that the clientele is mostly made up of Luxembourg residents and commuters working in the Grand-Duchy. Transactions occurred essentially face-to-face, with the exception of well-known bidders (where transactions were occasionally

[258] AED, *Rapport d'activité 2021 de l'Administration de l'enregistrement, des domaines et de la TVA,* 2021, link, 2022, link and 2023, link.

[259] 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.

[260] CdN data.

[261] The EUR 1 million listed item corresponded to a highly specialised industry machine.

performed over the phone). If intermediaries were used during auctions, proxy and BO verification were performed.

### 6.4.4. *Audit profession*[262,263]

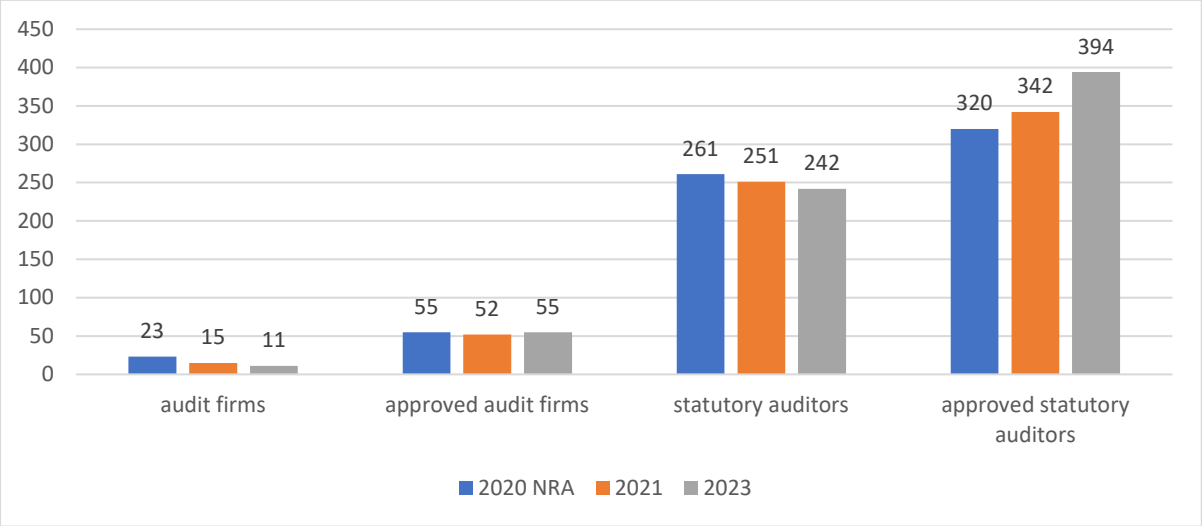
**AT A GLANCE**

The sub-sector inherent risk level is assessed as "Medium".

Sub-sector size, international exposure and significant number of audit clients are the key vulnerabilities driving ML inherent risk for the audit profession. With respect to the 2020 NRA, more detailed data available for the 2025 NRA update have shown that, for instance, TCSPs activities 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.

The following table provides an updated overview of the Luxembourg audit profession landscape.

**Figure 26: Evolution Luxembourg audit landscape**[264]




As depicted in the figure above, the sector remained sizable at end 2023. Over 90% of the total turnover of the audit profession is generated by the four largest audit firms with 55% of statutory auditors and 71% of statutory auditors in public practice working for these firms. The remaining 140 professionals in public practice work in 62 audit firms or are sole practitioners (8 of them). Consequently, the sector continued to be moderately fragmented throughout the observation period.

With respect to the ownership structure of (approved) audit firms, BOs and board members of the audit firms were resident in Luxembourg or in another EU country. In 2021 and 2023, none had a BO,

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

[263] Statistics collected by the IRE based on 2023 RBA questionnaire referring to the situation as at year end of 2023, unless stated otherwise.

[264] IRE data. "2020 NRA" data at 21 February 2020. As the last RBA questionnaire was communicated by statutory auditors at the end of 2023 / beginning 2024, 2023 figures (instead of 2022 statistics) were reported in the last RBA questionnaire.

shareholder or board member residing in a jurisdiction under increased monitoring by the FATF or a high-risk jurisdiction subject to a call for action[265].

Auditors' core activities relate to assurance services such as audit and review of annual accounts. These activities are considered to be low ML risk. Furthermore, 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 81% of the total turnover and 83% of their clients as a whole in 2023. TCSP activities, which are deemed to be higher risk from a ML point of view, represented a minor share of total activities (0,83% of auditors total turnover; provided to 1,4% of their clients in 2023 and 0,10% of total turnover and 1,4% of total clients in 2021). This decreases audit profession's vulnerability to ML related to products and services.

Auditors predominantly served a regional clientele with 92% (91%) of them being registered or residing in the "*Grande region*" in 2023 (2021). In a similar vein, BOs of audit firm clients were mainly resident in EU countries (68% in 2023, 72,5% in 2021), the UK (9,4% in 2023, 8% in 2021), the USA (8% in 2023, 6,5% in 2021) and Switzerland (6% in 2023 , 5% in 2021).

The number of clients amounted to around 34 700 in 2023 (34 600 in 2021) for the whole profession. (Approved) audit firms' clients were mainly represented by Luxembourg *sociétés commerciales* (84% in 2023 – 83% in 2021) from both the financial and non-financial sector[266]. Throughout the observation period, 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. The number of BOs of legal persons clients of the audit profession who were PEPs represented 3,4% of the total number of BOs reported by the audit profession in 2023.

### *6.4.5. Chartered professional accountants*

**AT A GLANCE**

Inherent risk related to CPAs remains high, with key risk drivers stemming from the profession's size, products and activities, international business as well as from their clientele.

During the observation period of this NRA, the sector remained large in size and fragmented, with on average around 1 200 of CPAs natural persons spread across 560 legal entities and 66 independent professionals. Around 30% of the professionals were employed by one of the six biggest firms. Although the sub-sector also included a significant number of small entities, their share of total revenue was limited and reserved to bigger entities. The number of large chartered professional accounting firms falling under the OEC AML/CFT supervision remained limited (with less than 2% of registered legal entities employing more than 250 persons). Most entities under the OEC supervision were small legal entities with around ¾ of them employing less than 11 persons[267].

Compared to the 2020 NRA, CPAs continued to play a key gatekeeper and intermediary role for many transactions presenting a high ML risk. Indeed, CPAs provide a significant amount of TCSPs activities, which are considered high risk from a ML perspective. However, a downward trend may be observed

[265] CSSF data.
[266] IRE data.
[267] OEC data.

through the observation period, notably among sole practitioners. Whilst the share of registered legal entities under OEC providing TCSP activities has slightly decreased from 71% in 2020 to 68% in 2023, the share of sole practitioners providing TCSP activities has diminished more significantly, from 51% in 2020 to 26% in 2023[268]. CPAs' high share of international business and volume and risk profile of clients further adds to this risk.

## 6.5. Legal persons and legal arrangements

The 2018 NRA and its 2020 update included a specific section on legal persons and legal arrangements. In both exercises, legal persons and legal arrangements as a whole were considered as highly vulnerable for ML/TF purposes. Luxembourg obtained a more granular understanding of Luxembourg legal persons and legal arrangements vulnerabilities through the LPs/LAs VRA[269], finalised and published in February 2022. The 2022 LPs/LAs VRA constitutes the common understanding of Luxembourg's legal persons and legal arrangements vulnerabilities for being abused for ML/TF purposes.

**Table 21: Inherent ML risk of legal persons and legal arrangements – overview by sub-sector**

| Sector | Sub-sectors | 2025 NRA: Inherent risk |
|---|---|---|
| Legal persons and legal arrangements | *Sociétés commerciales* | Very High |
| | *Sociétés civiles* | Medium |
| | NPOs (as per FATF definition) carrying out primarily international activities – ASBLs and *Fondations*[270] | High |
| | NPOs (as per FATF definition) carrying out local activities – ASBLs[271] | Low |
| | NPOs (as per FATF definition) carrying out local activities – *Fondations*[272] | Low |
| | Other legal persons | High |
| | Domestic *Fiducies* | Very High |
| | Foreign trusts | Very High |

[268] OEC data.

[269] MoJ, *Legal persons and legal arrangements ML/TF vertical risk assessment*, 2022, link.

[270] This category corresponds to "*Associations sans but lucrative* (ASBL) and *fondations* with Non-governmental organisations (NGO) status" in NRA 2020.

[271] This category corresponds to "Other *associations sans but lucratif* (ASBL)" in NRA 2020. Note than in NRA 2020, it included ASBLs in and out of the FATF NPO definition (i.e. 8 000 vs. 100 ASBLs falling in FATF NPO definition). In this respect, NRA 2020 noted that "most ASBLs are estimated to have a low exposure to ML/TF threats; but given their relatively high number, the inherent risk is evaluated as medium for the local ASBL sector as a whole until a national assessment of their activities will permit a more granular assessment, in line with a conservative approach".

[272] This category corresponds to "Other *fondations*" in NRA 2020. Note that in NRA 2020, it included *Fondations* in and out of the FATF NPO definition.

### 6.5.1. *Legal persons*

**AT A GLANCE**

SNRA

Overall, the SNRA assesses the ML risks related to legal persons as very significant, with the ML risk mainly stemming from the misuse of complex structures and control structures, often using shell and front companies[273], as well as misusing off-shore companies[274]. The SNRA also notes that the majority of cases that involved tax evasion, fraudulent investment schemes and fraud also utilized complex structures to conceal beneficial ownership.

The SNRA provides other key techniques that have been identified allowing legal persons to be exploited to hide beneficial ownership information, such as using individuals and financial instruments to obscure the relationship between the BO and the asset, including bearer shares, nominees, and professional intermediaries; falsifying activities through the use of false loans, false invoices, and misleading naming conventions, fictitious turnover; misuse of cash-intensive business to provide cover for the source of otherwise inexplicable quantities of cash, facilitating the mixing of illicit funds with legal proceeds; and use trade-based money laundering to justify the movement of criminal proceeds through banking channels, for example, via letters of credit and invoices, or through the use of global transactions, often using false documents for the trade of goods and services.

In connection to organised crime (see section 5.1.5), the SNRA suggests that where organised criminal groups have connections to a jurisdiction, they may seek to move illicit proceeds to and from that jurisdiction to facilitate offending, often in relation to drug offences.

NRA

The 2018 and 2020 NRA assessed the legal persons sector as "High" risk, with *Sociétés commerciales*, followed by some NPOs bearing the highest inherent risk. Following the 2025 NRA, the inherent risk levels remain roughly the same for all categories of legal persons (with the exception of "Other legal persons", assessed as High risk, in line with the 2022 LPs/LAs VRA, and ASBLs falling under FATF NPO definition carrying out local activities, that have been assessed as Low risk). Indeed, leveraging on the methodology developed in the 2022 LPs/LAs VRA and updated data, this NRA provides a more detailed, nuanced and data-based assessment.

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 146 373 (5% increase from 139 430 legal persons as of 31 December 2021), but it is still below the number observed in the years before the NRA 2020.

By broad category of legal persons, *Sociétés commerciales* increased the most, with 6 349 additional entities. Within this category, SARLs and SCSpé contributed the most to this increase with respectively

[273] Shell companies and front companies feature prominently in most complex structures identified by FIUs and other competent authorities, according to FAFT and Egmont Group, *Concealment of Beneficial Ownership, 2018,* link.

[274] According to the SNRA, offshore companies are often lacking real economic activity in the jurisdiction of incorporation. This, together with the high number of intra-affiliated-companies transactions, could increase the risk for such companies of being abused for ML.

4 071 and 3 234 additional entities. On the other hand, SAs decreased by 2 598 entities. *Sociétés civiles* increased by 223 to reach 6 068 entities. Within the non-profit sector, the number of *ASBLs* (out of which only a portion fall within the FATF NPO definition) increased by 349 to reach 8 806, while the number of *Fondations* remained stable at around 200. Other legal persons also remained fairly stable (just below 3 000, 2% of the total).

In terms of structure of the Luxembourg legal persons landscape, the situation has been rather stable for the last years with around 87% of *Sociétés commerciales*, 4% of *Sociétés civiles*, 6% of non-profit legal persons (*ASBLs* and *Fondations*) and 2% of other legal persons.

**Table 22: Luxembourg legal persons by category 2017-2023**

| | Situation date | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Legal Form | 31/12/2020 | P% | 31/12/2021 | P% | 31/12/2022 | P% | 31/12/2023 | P% |
| **Commercial Companies** | **121 918** | **88%** | **121 916** | **87%** | **126 485** | **88%** | **128 265** | **88%** |
| Société coopérative | 141 | 0% | 149 | 0% | 147 | 0% | 148 | 0% |
| Société coopérative organisée comme une SA | 114 | 0% | 114 | 0% | 132 | 0% | 138 | 0% |
| Société anonyme | 36 533 | 26% | 32 392 | 23% | 31 110 | 22% | 29 794 | 20% |
| Société à responsabilité limitée | 73 226 | 53% | 74 461 | 53% | 77 531 | 54% | 78 532 | 54% |
| Société à responsabilité limitée simplifiée | 3 284 | 2% | 4 150 | 3% | 4 801 | 3% | 5 343 | 4% |
| Société par actions simplifiée | 185 | 0% | 212 | 0% | 249 | 0% | 273 | 0% |
| Société européenne | 41 | 0% | 56 | 0% | 55 | 0% | 51 | 0% |
| Société en commandite par actions | 1 951 | 1% | 2 087 | 1% | 2 218 | 2% | 2 326 | 2% |
| Société en commandite simple | 1 697 | 1% | 1 849 | 1% | 1 955 | 1% | 1 997 | 1% |
| Société en commandite spéciale | 4 579 | 3% | 6 304 | 5% | 8 148 | 6% | 9 538 | 7% |
| Société en nom collectif | 167 | 0% | 142 | 0% | 139 | 0% | 125 | 0% |
| **Civil Companies** | **5 478** | **4%** | **5 845** | **4%** | **6 065** | **4%** | **6 068** | **4%** |
| Société civile | 5 478 | 4% | 5 845 | 4% | 6 065 | 4% | 6 068 | 4% |
| **ASBLs** | **8 504** | **6%** | **8 457** | **6%** | **8 717** | **6%** | **8 806** | **6%** |
| Association sans but lucratif | 8 504 | 6% | 8 457 | 6% | 8 717 | 6% | 8 806 | 6% |
| **Fondations** | **218** | **0%** | **193** | **0%** | **192** | **0%** | **193** | **0%** |
| Fondation | 218 | 0% | 193 | 0% | 192 | 0% | 193 | 0% |
| **Other legal persons** | **3 096** | **2%** | **3 019** | **2%** | **3 027** | **2%** | **3 041** | **2%** |
| Association d'Assurance Mutuelle | 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% |
| Société créée selon la loi du 24 mars 1989 | 1 | 0% | 1 | 0% | 1 | 0% | 1 | 0% |
| Société d'investissement à capital variable | 1 175 | 1% | 1 136 | 1% | 1 099 | 1% | 1 080 | 1% |
| Société européenne d'investissement à capital variable (SICAV-SE) | 1 | 0% | 1 | 0% | 1 | 0% | 1 | 0% |
| Groupement d'intérêt économique | 80 | 0% | 82 | 0% | 88 | 0% | 92 | 0% |
| Groupement européen d'intérêt économique | 59 | 0% | 58 | 0% | 60 | 0% | 59 | 0% |
| Association agricole | 110 | 0% | 86 | 0% | 88 | 0% | 88 | 0% |
| Association épargne-pension | 10 | 0% | 10 | 0% | 10 | 0% | 11 | 0% |
| Etablissement public | 118 | 0% | 123 | 0% | 128 | 0% | 131 | 0% |
| Fonds commun de placement | 1 530 | 1% | 1 505 | 1% | 1477 | 1% | 1461 | 1% |
| Fonds d'investissement alternatif réservé | 2 | 0% | 2 | 0% | 2 | 0% | 2 | 0% |
| Mutuelle | 3 | 0% | 8 | 0% | 18 | 0% | 32 | 0% |
| Fonds de titrisation | - | 0% | - | 0% | 48 | 0% | 76 | 0% |
| Total | 139 214 | 100% | 139 430 | 100% | 144 486 | 100% | 146 373 | 100% |

The ability to be used as complex structures is a key vulnerability of legal persons. 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 exposure to ML risk.

**Basic information registered in the RCS** shows that corporate owners were more prevalent in *Sociétés commerciales* than in *Sociétés civiles*[275].

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

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

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%[276].

Non-resident shareholders/partners: as analysed in the 2022 LPs/LAs VRA, and according to the information on addresses for registered shareholders/partners within the corporate structure, it appears that *Sociétés commerciales* bear a higher vulnerability than *Sociétés civiles*[277].

**BO information**[278] of legal persons must be registered with the *Registre des bénéficiares effectifs* (RBE) as per the 2019 RBE Law. As of end 2023, 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*[279].

Information registered with the RBE as of 31 December 2023 confirms the international nature of BOs in the corporate environment in Luxembourg (see section 3), 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, *Fondations* and *Sociétés civiles*. *Sociétés commerciales* 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 commun de placements* (FCPs[280]).
  - Non-resident BOs in S*ociétés commerciales* represented a significant share, driven by the presence of non-resident BOs and *Sociétés anonymes (*62% of non-residents) and in *Sociétés à responsabilité limitées* (47% of non-residents)*,* which were the most prevalent legal forms of *Société commerciale* in Luxembourg.
  - For the remaining types of legal persons, BOs are mostly national residents.

With respect to **products and activities**, the following table summarises the sectoral activity split per category of legal person.

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

[277] MoJ, *Legal persons and legal arrangements ML/TF vertical risk assessment*, 2022, link.

[278] Note that in the following section, SMOs are included in BO statistics unless otherwise specified.

[279] Data provided by the LBR. Closed bankruptcies are not taken into account.

[280] 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 23: Sectoral split of legal persons as of 31 December 2023 (registered with RCS and NACE code allocation) – top-three sector per category highlighted in orange[281]**

| Sector | *Sociétés commerciales* | *Sociétés civiles* | *ASBLs* | *Fondations* | Other legal entities |
|---|---|---|---|---|---|
| Agriculture, forestry and fishing | 189 | 121 | 7 | - | 33 |
| Mining and quarrying | 13 | - | - | - | - |
| Manufacturing | 922 | 3 | 3 | - | 3 |
| Electricity, Gas, Steam and Air Conditioning supply | 204 | 141 | 1 | - | 8 |
| Water supply | 67 | - | 2 | - | 14 |
| Construction | 7 005 | 36 | | - | 3 |
| Wholesale and retail trade | 9 772 | 7 | 2 | - | 17 |
| Transportation and storage | 1 655 | 4 | 1 | - | 3 |
| Accommodation and food service activities | 3 652 | 5 | 19 | - | - |
| Information and communication | 3 475 | 1 | 93 | 1 | 18 |
| Financial and insurance activities | 70 915 | 437 | 8 | 1 | 2 177 |
| Real estate activities | 5 411 | 3 442 | 5 | 2 | 12 |
| Professional, scientific and technical activities | 9 060 | 70 | 74 | 4 | 43 |
| Administrative and support service activities | 3 348 | 710 | 79 | - | 14 |
| Public administration and defence | 2 | - | 35 | 3 | 46 |
| Education | 567 | 3 | 145 | 10 | 12 |
| Human health and social work activities | 522 | 14 | 533 | 39 | 45 |
| Arts, entertainment and recreation | 486 | 33 | 2 074 | 7 | 15 |
| Other service activities | 1 303 | - | 4 610 | 82 | 28 |
| Activities of extraterritorial organisations and bodies | 1 | - | 1 | | - |

[281] Note that as of Q3 2024, the NACE Code allocation for some legal persons (about 8%) 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 2023 (i.e. 146 373) with the RCS. Nonetheless, it is considered that this does not impact the overall structural split shown above.

From the table above, it can be concluded that more than 55% of *Sociétés commerciales* are active in the financial and insurance sector, which is in line with Luxembourg's context (see section 3). *Sociétés commerciales* are far less active in other sectors in percentage terms (wholesale and retail trade: 7,6%); professional, scientific and technical activities: 7%; construction activities: 5,5%) but still important in terms of number of entities[282].

More than half of *Sociétés civiles* are largely active in real estate activities[283], which is globally considered high risk from a ML perspective.

With regard to the non-profit sector, it is worth noting that the information in the table above concerns all ASBLs and *Fondations* registered with the RCS. Taking into consideration those identified to fall under FATF Recommendation 8 definition as "NPOs", it can be observed that those that were engaged in international activities were mainly active in development (economic, social, education, etc.) and humanitarian relief aid; whereas those that were engaged primarily nationally were primarily active in social work without accommodation, religious (although most of them related to the financing of buildings or church organs in Luxembourg), and cultural activities. Those NPOs engaging both domestically and abroad were mostly active in social work without accommodation, development and humanitarian works, and cultural activities[284].

Other legal persons were mostly active in the financial and insurance sector[285], which is explained by the fact that FCPs and SICAVs used in the collective investment industry are included in this broad category.

### *6.5.2. Legal arrangements*

**AT A GLANCE**

**SNRA**

Overall, the SNRA assesses the ML risks related to legal arrangements as very significant.

Similar to legal persons, trusts and similar legal arrangements may be misused in order to increase opacity within ML. Moreover, the SNRA points out that in the case studies presented, almost all of the cases involving the use of legal arrangements also involve company or other legal entities, indicating that trusts and similar legal arrangements are rarely used in isolation to hold assets and obscure BOs, but they are generally part of a wider scheme, often involving tax crimes (see for instance section 5.1.2).

**NRA**

The 2018 and 2020 NRA assesses legal arrangements as "Very High" risk. Following the 2025 NRA, the inherent risk levels remain roughly the same for both domestic *fiducies* and foreign trusts. However,

[282] Note that for 7,6% of *Sociétés commerciales* as of 31 December 2023 NACE codes are unknown.

[283] Note that for 17% of *Sociétés civiles* as of 31 December 2023 NACE codes are unknown.

[284] Outcomes from the desktop analyses performed as of end 2022 and end 2023 by the LBC/FT Directorate of the Ministry of justice to identify NPOs that fall within the FATF 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.

[285] Note that for 16% of Other legal persons as of 31 December 2023 NACE codes are unknown.

leveraging on the methodology developed in the 2022 LPs/LAs VRA, the 2025 NRA provides a more detailed, nuanced and data-based assessment.

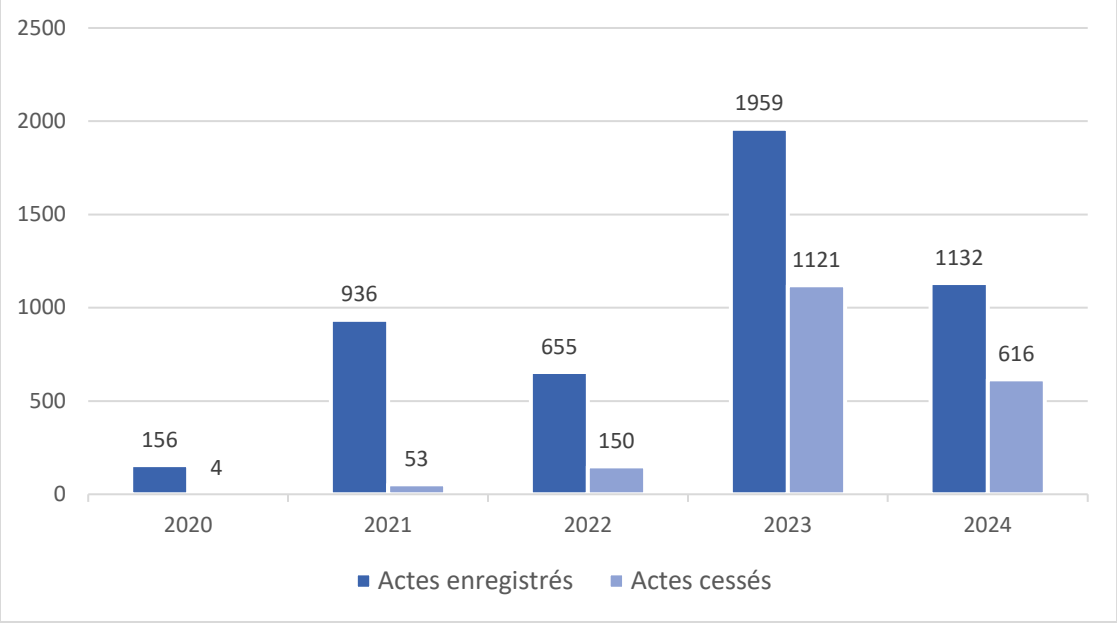
Key risk drivers are ownership/legal structure (referring to beneficial ownership and legal features of legal arrangements) and product and services, followed by sub-sector structure (size).

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[286]. However, this characteristic of legal arrangements may be abused for ML purposes. As explained above, legal arrangements have been identified as a recurring vehicle used in ML schemes globally[287].

In Luxembourg, legal arrangements comprised domestic *fiducies* and foreign trusts[288]. Except for the number of entities, both *fiducies* and foreign trusts shared the same key vulnerabilities to ML.

The register of *fiducies* and trusts (RFT) went live in the second half of 2020. The graph below shows the evolution of legal arrangements registered *"actes enregistrés"* and ceased *"actes cessés"* during the year and the following table and shows the number of legal arrangements active at year end. The below figure 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 27: RFT registrations over the period 2020 - 2024**




[286] MoJ, *Legal persons and legal arrangements ML/TF vertical risk assessment*, 2022, link (section 5.1.2.2).

[287] 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.

[288] A detailed description, examples and related key legislation is provided in the LPs/LAs VRA, section 3.4 (pages 23-25), link.

**Table 24: RFT registrations over the period 2020 - 2024[289]**

| 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** |

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)[290].

Generally, it is allowed 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[291]. From a geographical point of view, beneficial ownership structure is diverse[292]. Nevertheless, there were no BO resident in a high-risk jurisdiction subject to a call for action by FATF[293].

## 6.6. Cross-cutting vulnerabilities

### *6.6.1. Trust and corporate service providers (TCSPs)*

The 2004 AML/CFT Law (as amended by the Law of 29 July 2022) defines TCSPs as any natural or legal person which by way of a business relationship provides any trust and corporate services to third parties. There is no specific license for TCSPs. Instead, TCSPs are defined by the activities they perform.

The table below maps the five TCSP services as described in the 2004 AML/CFT Law to the description of the respective service as per the FATF definition described in FATF's "Guidance for a Risk-Based Approach for Trust & Company Service Providers (TCSPs)".

[289] AED.
[290] AED.
[291] OECD – IDB, A beneficial Ownership Implementation Toolkit, 2019, page 12.
[292] Data from the RFT as of 31 December 2024.
[293] FATF, High-Risk Jurisdictions subject to a Call for Action - 25 October 2024, link.

**Table 25: Mapping of TCSP activities described in the 2004 AML/CFT Law to the FATF Guidance on TCSPs**

| TCSP services described in the 2004 AML/CFT Law[294] | | Mapping to the FATF definition[295] |
|---|---|---|
| a) | Forming companies or other legal persons | **Incorporation:** Acting as a formation agent of legal persons |
| b) | Acting as or arranging for another person to act as a director, manager, member of the board of directors, member of the Executive Board or secretary of a company, a partner of a partnership, or a similar position in relation to other types of legal persons | **Directorship and secretarial services:** Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons |
| c) | Providing a registered office, business address, correspondence or administrative address or business premises and, where applicable, other related services for a company, a partnership or any other legal person or legal arrangement | **Domiciliation:** Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement |
| d) | Acting as, or arranging for another person to act as, a *fiduciaire* in a *fiducie*, a trustee of an express trust or an equivalent function in a similar legal arrangement | ***Fiducie/*trust**: Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement |
| e) | Acting as, or arranging for another person to act as, a nominee shareholder for another person | **Nominee shareholder:** Acting as (or arranging for another person to act as) a nominee shareholder for another person |

A range of professions in Luxembourg conduct at least one (or more) of the activities defined by the 2004 AML/CFT Law as TCSP activities (as described above). Entities that act as TCSPs include, amongst others, banks, investment firms, specialised PFSs, IFMs, PSAs, lawyers, audit professionals[296] and CPAs. Luxembourg notaries and bailiffs do not provide TSCP services[297]. The activity of domiciliation is regulated by the Law of 31 May 1999 governing the domiciliation of companies, as amended (1999 Domiciliation Law), and restricted to credit institutions, PFSs, PSAs, lawyers, auditors and CPAs. TCSPs are thus a broad and diverse category in Luxembourg, given the range of professionals that are legally authorised to conduct such activities.

The table below describes the professions authorised to carry out TCSP activities in Luxembourg, the relevant laws that underpin them and their respective AML/CFT supervisor.

[294] Article 1(8) of the 2004 AML/CFT Law, as amended by the Law of 29 July 2022.

[295] FATF, *Guidance for a Risk-Based Approach for Trust & Company Service Providers (TSCPs)*, 2019, link.

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

[297] MoJ, *ML/TF vertical risk assessment on legal persons and legal arrangements,* 2022, link (section 5.4.1.).

**Table 26: Professionals authorised to carry out TCSP activities in Luxembourg**

| AML/CFT supervisor | Professionals authorised to carry out TCSP activities | Relevant laws |
|---|---|---|
| **CSSF** | Banks and credit institutions | 1993 LSF, Part I, Chapter 1 |
| | Investment firms | 1993 LSF, Part I, Chapter 2, Section 2, Subsection 1 |
| | Investment Fund managers | 2010 OPC Law[298] and 2013 AIF Law[299] |
| | Securitisation undertakings | 2004 Securitisation Law[300], 2004 AML/CFT Law, Art. 2(1) 6b |
| | Three types of specialised PFSs[301], including with the following licenses: | |
| | • Family Offices | 1993 LSF, Art. 28-6 |
| | • Corporate domiciliation agents | 1993 LSF, Art. 28-9 |
| | • Professionals providing company incorporation and management services | 1993 LSF, Art. 28-10 |
| **CAA** | Professionals of the insurance sector | 2015 Insurance Law[302], Art. 264, 265 and 266 |
| **OEC** | CPAs | 1999 Chartered Professional Accountants Law[303]; 1999 Domiciliation Law, Art. 1(1)[304] |
| **IRE** | (Approved) statutory auditors and (approved) audit firms | 2016 Audit Profession Law[305] |
| **OAL/OAD** | Lawyers (list I and IV of the Bar) | 1991 Lawyers Law[306] |
| **AED[307]** | Other professions offering TCSP services: | 2004 AML/CFT Law, Art. 2-1, para. 8 |
| | • Professional directors supervised by the AED | |
| | • Business centres | |

[298] Law of 17 December 2010 relating to undertakings for collective investment.

[299] Law of 12 July 2013 on alternative investment fund managers.

[300] Law of 22 March 2004 on securitisation.

[301] Including support professionals of the financial sector providing TCSP services.

[302] Law of 7 December 2015 on the insurance sector.

[303] Law of 10 June 1999 organising the profession of Chartered Professional Accountant.

[304] Based on the professionals listed in the Law of 31 May 1999 (1999 Domiciliation Law), Art. 1(1): "Only a registered member of one of the following regulated professions established in the Grand-Duchy of Luxembourg may act as a domiciliation agent of companies: a credit institution or another professional of the financial sector and the insurance sector, an lawyer at the Court (*avocat à la Cour*) included in list I and a European lawyer practising under his home-title professional title included in list IV referred to in Art. 8(3) of the amended Law of 10 August 1991 on the profession of avocat, *réviseur d'entreprises* (statutory auditor), *réviseur d'entreprises agréé* (approved statutory auditor) or accountant".

[305] Law of 23 July 2016 concerning the audit profession.

[306] Law of 10 August 1991: List I lawyers defined as lawyers at the Court (*avocat à la Cour)* who are fully qualified Luxembourg lawyers; List IV lawyers defined as EU admitted lawyers (*avocat de l'UE exerçant sous son titre d'orgine)* who are foreign lawyers from the European Union practising under their original professional title.

[307] These other professions have business associations – *Association luxembourgeoise des centres d'affaires* (ALCA) and *Institut luxembourgeois des administrateurs* (ILA) – but membership is optional and these associations are not SRBs.

As noted in the 2020 NRA, the nature of the services offered may also differ significantly between different types of professionals. The nature of domiciliation services performed by asset managers differs from those of specialised PFSs (i.e., the former focusing on the creation of special purpose vehicles to separate investments from client assets). Investment Fund managers only provide domiciliation services to entities linked to them. They do not provide third-party domiciliation. Similarly, PSAs can only provide domiciliation services to insurance undertakings under the CAA supervision or to companies belonging to the same group as the latter.

In addition, while many professions can offer TCSP activities, not all of them do so in practice (some only offer or conduct a subset of activities). As shown in the Insight Box below, even though (approved) statutory auditors are legally authorised to conduct TCSP activities, only a minor share does so in practice.

**Insight Box 15: TCSP activities provided by IRE members**

The activity of the IRE's members is predominantly focused on audit and assurance services. Some IRE members may provide TCSP activities presenting higher risks from an ML perspective. In order to gain a better understanding of the nature and extent of those activities, the IRE included specific questions in their annual risk-based approach questionnaire (RBA questionnaire).

**Table 27: Breakdown of TCSP services offered by the audit profession (2023 RBA Questionnaire data)**

| Services rendered by IRE members | Number of clients for which those services were rendered (% for the audit profession) | Turnover generated by these services (% for the audit profession) |
|---|---|---|
| Incorporation of companies and trusts[308] | 0,62% | <0,83% |
| Board of Directors' mandates | 0,20% | |
| Domiciliation services | 0,59% | |
| Companies' management and services rendered to trusts or fiduciaries | 0% | |
| Carrying shareholder | 0% | |

Considering the figures above, among the IRE members that perform TCSP activities, most of them offer domiciliation services and assistance for the setting-up of companies including assistance provided for licensing or registering companies with authorities. Nevertheless, the extent (number of clients serviced and turnover generated) is very limited.

The Insight Box below provides a detailed view about TCSPs activities conducted by OEC members.

[308] Including the assistance for the setting-up of companies, the assistance provided for licensing or registering companies with authorities.

**Insight Box 16: TCSP activities provided by OEC member firms**

While some OEC member firms might also offer TCSP services, their number is relatively small as shown in the table below (2024 RBA questionnaire regarding 2023 data).

**Table 28: Breakdown of TCSP services offered by OEC member firms**

| Services rendered by OEC member firms | % performing this activity | % of turnover | | | |
|---|---|---|---|---|---|
| | | >75% | 10–75% | <10% | Not applicable |
| Company formation services or other legal entity services | 29,41% | 0% | 0,71% | 10,35% | 88,94% |
| Director or a similar function in respect to other legal entities | 36% | 1,88% | 9,41% | 16,94% | 71,76% |
| Domiciliation without director's mandate | 41,41% | 0% | 7,53% | 22,59% | 69,88% |
| Domiciliation with director's mandate | 33,65% | 0,24% | 6,82% | 19,29% | 73,65% |
| Office rental-business centre | 17,65% | 0,47% | 3,29% | 10,59% | 85,65% |
| Fiduciary contracts | 0,24% | 0% | 0% | 0% | 100% |
| Trustee in an express trust | 0,71% | 0,24% | 0% | 0,24% | 99,53% |
| Other[309] | 0,71% | 0% | 0% | 0% | 100% |

Given the relatively low number of sole practitioners offering TCSP services, the table above only highlights the respondent firms providing TCSP services. At first glance, domiciliation services seem to be the most prevalent TCSP offering; however, for the firms who do provide this service, the revenue generated from it is relatively minor, often representing 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.

The following table provides an overview of the TCSP landscape in Luxembourg.

[309] For instance, equivalent function (as fiduciary or trustee) in a similar structure, etc.

**Table 29: TCSPs – Overview of professions performing TCSP activities, 2023**

| Supervisor | Professionals | TCSP activity that may be performed (as defined in the 2004 AML/CFT Law) | | | | | |
|---|---|---|---|---|---|---|---|
| | | Sector size: # of entities[310] | Sector size: # of entities offering TCSP services | Incorporation | Directorship and secretarial | Domiciliation | *Fiducie*/trust[311] |
| **CSSF** | Banks and credit institutions | 120 | 28 | ✔ | ✔ | ✔ | ✔ |
| | Investment firms | 92 | 13 | ✔[312] | ✔[313] | ✔[314] | ✔ |
| | Investment Fund managers | 1 212 | 198[315] | ✔ | ✔ | ✔[316] | ✔ |
| | Regulated Securitisation undertakings[317] | 2 | 2 | | | | ✔ |
| | Specialised PFSs: Professionals providing company incorporation and management services | 100[318] | 85[319] | ✔ | ✔ | | ✔[320] |
| | Specialised PFSs: Corporate domiciliation agents | | | ✔ | ✔ | ✔ | ✔[321] |

[310] Where no disctinction can be made between professionals that do and those that do not perform TCSP activities, this number reflects the total number of professionals in the sub-sector as indicated in section 6; otherwise, it is specified.

[311] Acting as, or arranging for another person to act as a *fiduciaire* in a fiducie, a trustee of an express trust or an equivalent function in a similar legal arrangement.

[312] An investment firm must hold a "Professionals providing company incorporation and management services" license to provide incorporation services.

[313] An investment firm must hold a "Professionals providing company incorporation and management services" license, a "Domiciliation agent" license or a "Family Office" license to provide directorship and secretarial services.

[314] An investment firm must hold a "Domiciliation agent" license to provide domiciliation services.

[315] Only for entities which are related to them (e.g. Special Purpose Vehicle for Private equity funds). No third party domiciliation.

[316] The Management companies only provide domiciliation services to entities linked to them. No third party domiciliation.

[317] Undertakings when they perform TCSP activities (refer to Art. 2(1) 6b) of the 2004 AML/CFT Law).

[318] Including all entities under the AML/CFT supervision of the Specialised PFS department.

[319] Including one support PFS providing TCSP services.

[320] Specialised PFSs are authorised to provide trust services, but cannot act as *fiducie* under Law of 27 July 2003 on *Fiducies* and Trusts, Art. 4.

[321] Specialised PFSs are authorised to provide trust services, but cannot act as *fiducie* under Law of 27 July 2003 on *Fiducies* and Trusts, Art. 4.

| Supervisor | Professionals | TCSP activity that may be performed (as defined in the 2004 AML/CFT Law) | | | | | |
|---|---|---|---|---|---|---|---|
| | | Sector size: # of entities[310] | Sector size: # of entities offering TCSP services | Incorporation | Directorship and secretarial | Domiciliation | *Fiducie*/trust[311] |
| | Specialised PFSs: Family offices | | | [322] | ✔ | [323] | ✔ [324] |
| **CAA** | PSAs | 26 | 13 | | ✔ | ✔ | |
| **OEC** | CPAs | 1 232 | 382 | ✔ | ✔ | ✔ | ✔ |
| **IRE** | Audit firms | 66 | 14[325] | ✔ | ✔ | ✔ | ✔ [326] |
| | Sole practitioners | 8 | 5[327] | | ✔ | ✔ | |
| **OAL/OAD** | Lawyers | 3 296 (OAL) | 13 | ✔ | ✔ | ✔ | ✔ [328] |
| | Lawyers' offices | 758 (OAL) | 98 | | | | |
| **AED** | Business centres | 66 | 66 | | ✔ | | |
| | Professional directors | 220-230 | 220-230 | | ✔ | | |

[322] A Family Office must also hold a "Professionals providing company incorporation and management services" to provide incorporation services.

[323] A Family Office must also hold a "Domiciliation agent" license to provide domiciliation services.

[324] Specialised PFSs are authorised to provide trust services, but cannot act as *fiducie* under Law of 27 July 2003 on *Fiducies* and Trusts, Art. 4.

[325] Based on annual declarations as at December 31, 2023.

[326] Note that in practice this activity is not provided, as reported in Table 27.

[327] Based on annual declarations as at December 31, 2023.

[328] Can assist clients being fiduciaries or managing a *fiducie* themselves.

In order to have a more granular view of the risks stemming from services provided by TCSPs, the following sub-sections provide a more granular analysis on the different types of services.

#### *6.6.1.1. Incorporation services*

Professionals that provide services to third parties relating to the formation of companies or any other legal person are considered to provide incorporation services.

As noted in the Concealment of Beneficial Ownership joint report of FATF and the Egmont Group[329], criminals often misuse legal persons as a vehicle to hide the origin of their funds or/and their real identity.

Under Luxembourg's law, there is no requirement for a TCSP to be directly involved in a company's incorporation. The nature of ML risks relating to the provision of these services is related to the ways in which a criminal may abuse or misuse this service to set up a complex network of structures that permits the concealment of their identity and the source of the funds.

As noted previously in 6.4.2, around two thirds of all Luxembourg legal persons were registered by notarial deed during the observation period of this analysis. Regardless of whether the transactions were prepared by other professionals (such as TCSPs), the scope and the rationale of the AML/CFT checks carried out by the Luxembourg notaries do not change. Indeed, professionals subject to the 2004 AML/CFT Law are required to perform CDD and BO controls in an independent manner and they should not rely on information conveyed by other professionals. This decreases ML risks related to incorporation services to some extent.

**Insight Box 17: CSSF entities providing incorporation services**

As of 31 December 2023, incorporation services were provided by the following CSSF supervised entities:

- 6 out of 120 banks (5%);
- 58 out of 100 specialised PFS (58%);
- 5 out of 92 investment firms (5%); and
- 92 out of 1 212 Investment Fund managers (8%) offer incorporation services.

#### *6.6.1.2. Directorship and secretarial services*

Secretarial services are typically less vulnerable to ML. They generally involve the execution of back-office activities that have limited overlap with actions typically carried out with the purpose of laundering illicit funds. Nevertheless, clients maintain responsibility over decisions and actions executed by the structure. As such, clients or their BOs will be recorded as the originator or approver of decisions, hence limiting the opportunities to conceal their identity. Therefore, potential for administration services to be abused or misused for ML purposes is limited, compared to setup and management services. Still, while relatively

[329] Egmont-FATF Joint Report, *Concealment of Beneficial Ownership,* 2018. See section 1 for an overview and section 3 with regards to incorporation services, particularly paragraphs 121 to 125, 130 to 135, 141 to 145 and 152 to 156, link.

limited, there may be instances, such as the use of administrative services to give substance to the company, in which criminals are able to abuse or misuse administration services provided by TCSPs[330].

As stated in the 2022 LPs/LAs VRA any appointed director (natural or legal persons acting on its own account or on behalf of a client) must be registered with the RCS[331]. As a consequence, the registered director is fully liable under Luxembourg civil and criminal law, and thus has the incentive to ensure an appropriate level of controls are applied over actions and transactions they are approving. This drastically reduces the level of exposure to ML risk.

**Insight Box 18: CSSF entities providing directorship and secretarial services**

As of 31 December 2023, the following CSSF supervised entities offered directorship and secretarial services:

- 17 out of 120 banks (14%);
- 74 out of 100 specialised PFS (74%);
- 9 out of 92 investment firms (10%); and
- 139 out of 1 212 Investment Fund managers (11%).

#### *6.6.1.3. Domiciliation services*

Whereas the 2004 AML/CFT Law defines a range of professionals that can carry out TCSP activities, the activity of domiciliation services is further regulated by the 1999 Domiciliation Law. More precisely, this law allows a company (the "domiciled company") to establish a seat (a registered office) with a third party (the "domiciliation agent") in order to carry out an activity within the framework of the domiciled company's corporate purpose. The same law states that the domiciliation agent may also provide other services related to the activity of the domiciled company (the "domiciliation services"). Finally, the law requires that the domiciled company and the domiciliation agent should conclude a written agreement called a domiciliation contract.

As such, domiciliation services are a type of business that provides third parties with a seat and ancillary services (directorship services, corporate secretariat, accounting services, holding of general meetings, provision of office space, etc.) for a company.

Domiciliation services respond to a broad number of needs and they are often used together with other corporate services. For instance, TCSPs may offer domiciliation services complementing their specialised advice services in legal, commercial and tax matters. Furthermore, not all companies may find it cost effective to own or rent private premises. A company can therefore be "domiciled" at a lower cost on the premises of a domiciliation agent.

However, this particular possibility for establishing a registered office is not suitable for operational companies with a commercial, craft or industrial activity. Indeed, any operational company established in Luxembourg is required to obtain a business license from the MoE in accordance with the Law of 2

[330] MoJ, *National risk assessment on money laundering and terrorist financing,* 2020, link.
[331] MoJ, *Legal persons and legal arrangements ML/TF vertical risk assessment*, 2022, link.

September 2011 regulating the access to different professions of craftsman, trader, industrialist, as well as to certain liberal professions (2011 Business Licenses Law), which specifically states that domiciliation within the meaning of the 1999 Domiciliation Law does not constitute an establishment[332], and therefore cannot use such domiciliation services.

Pursuant to articles 100-2 and 1300-2 of the Law of 10 August 1915 (1915 Companies Law), domiciled companies (provided the domiciliation contract offers a registered office to the company) must make key decisions (e.g. strategic, financial or investment) in Luxembourg. Furthermore, pursuant to article 100-2 of the 1915 Companies Law, the domicile of a company is located at its central administration.

The 1999 Domiciliation Law is strict and only allows registered members of one of the following regulated professions established in Luxembourg to act as a domiciliation agent of companies: a credit institution or another professional of the financial sector and the insurance sector, a lawyer at the Court (*avocat à la Cour*) registered with List I and a European lawyer practising under the professional title of their home country registered with List IV, an (approved) statutory auditor or a CPA.

The IRE and the OEC require (approved) statutory auditors and CPAs to perform at least one of the following services, as required by professional standards, should they provide domiciliation services to another company:

- bookkeeping;
- preparation of financial statements and/or consolidated accounts;
- preparation of tax returns;
- mandate of *Commissaire* according to article 443-2 of the 1915 Companies Law; or
- directorship services.

In such situations, these TCSPs are registered as directors or managers at the RCS and thus become liable under the 1915 Companies Law, as well as under civil and criminal law (cf. section 6.6.1.2).

Furthermore, the CSSF for example issued different circulars dealing, amongst others, with the professional obligations of domiciliation agents, the minimum content required for a domiciliation agreement and precisions concerning the concept of "seat"[333].

All persons who can carry out domiciliation of companies are subject to the 2004 AML/CFT Law. As such, domiciliation agents are required to strictly comply with all the obligations set out in said law (e.g. identification of the client, application of a risk-based approach). The supervisory authorities and SRBs are responsible for verifying whether the professionals under their supervision comply with these obligations.

Pursuant to article 2 of the 1999 Domiciliation Law and as already touched on before, any person exercising the profession of domiciliation agent is subject to a number of obligations. For example,

[332] 2011 Business Licenses Law, article 5.

[333] CSSF, Circular CSSF 01/47 on Professional obligations of domiciliation agents of companies and general recommendations, amending Circular CSSF 01/28, 2001, link, Circular CSSF 02/65 on Law of 31 May 1999 governing the domiciliation of companies, precisions as regards to the concept of "seat", 2002, link. *Communiqué: Domiciliation activity exercised when operating a business centre or a co-working space,* 2021, link.

domiciliation agents must ensure that the domiciled company complies with the provisions of the 1915 Companies Law. Failure to comply with their obligations carries criminal sanctions. Article 4 of the 1999 Domiciliation Law provides for criminal penalties which include imprisonment ranging from eight days up to five years and a fine of between EUR 1 250 and EUR 12 000.

**Insight Box 19: OAL 2021 study on TCSP activities among their members**

The OAL published in September 2021 a detailed analysis of the TCSP activities performed by their members (data extracted from the off-site AML/CFT inspection in December 2020). The analysis revealed that TCSP activities accounted for less than 5% of their members' activities, with most of them providing domiciliation services.

With regard to domiciliation activities, 146 members stated that they performed such activities. More precisely,

- 66% of them indicated that they perform these services for less than 10 clients (i.e., legal persons);
- 22% of them indicated that they perform these services for 11 to 25 clients (i.e., legal persons);
- 8% of them indicated that they perform these services for 26 to 50 clients (i.e., legal persons); and
- 4% of them indicated that they perform these services for more than 50 clients (i.e., legal persons) – with only one lawyer stating that he domiciled more than 100 clients.

The analysis concluded that the share of the members' turnover related to domiciliation activities was rather limited. More precisely:

- 45% stated that the turnover related to these activities did not reach EUR 10 000;
- 33% stated that the turnover related to these activities was situated between EUR 10 000 and EUR 50 000;
- 9% stated that the turnover related to these activities was situated between EUR 50 000 and EUR 100 000;
- 7,5% stated that the turnover related to these activities was situated between EUR 100 000 and EUR 200 000; and
- 5,5% stated that the turnover related to these activities exceeded EUR 200 000.

Based on the analysis performed, the OAL concluded that TCSP activities were rather limited and that domiciliation services provided were generally overestimated. As revealed in the OAL annual AML/CFT questionnaires, the number of lawyers offering such services is decreasing.

The complete study can be found on the OAL's website (barreau.lu): link

#### 6.6.1.4. Nominee shareholder services

As the FATF explains in its Guidance for a Risk-Based Approach for Trusts and Company Service Providers[334], a nominee shareholder is a "[…] natural or legal person who is officially recorded in the Register of members (shareholder) of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the beneficial owner"[335].

Generally, the role of the nominee shareholder is to legitimately protect the identity of the BO and/or the controller of a company or asset. From a transparency standpoint, the involvement of nominee shareholders may contribute to obfuscate the identity of the BOs or, in exceptional cases, be used to circumvent jurisdictional controls on company ownership[336].

The Anglo-Saxon concept of "nominee shareholder" does not exist in Luxembourg civil and commercial law[337,338].

#### 6.6.1.5. Acting as a fiduciaire in a fiducie or as a trustee in a trust

The use of professional intermediaries or TCSPs is considered a key feature of the ML and broader organised crime environment[339]. As for professionals providing directorship or secretarial services, TCSPs acting as a *fiduciaire* in a *fiducie* or as a trustee in a trust might, un- or wittingly, be abused by criminals. Furthermore, the 2022 LPs/LAs VRA assessed both the inherent and residual risk of legal arrangements (and more specifically of *fiducies*) as "Very high"[340].

Nonetheless, it is worth mentioning that Luxembourg requires *fiduciaries* and trustees, as defined in the Law of 10 July establishing a Register of *Fiducies* and Trusts (2020 RFT Law), to obtain and keep at the place of administration of the express trust or *fiducie*, information on the BOs of any express trust administered in Luxembourg and of any *fiducie* for which they act as trustee or *fiduciaire* (article 2 of the 2020 RFT Law). On top of this requirement, article 13 of the 2020 RFT Law requires every *fiducie* or express trust of which a trustee or *fiduciaire* is established or resides in Luxembourg to submit detailed information on all BOs to the RFT. This register is maintained by the AED. The registration requirement also extends to legal arrangements whose trustees or *fiduciaires* are not established in Luxembourg or in any other EU Member State, but who enter into a business relationship or who acquire real estate in the

[334] FATF, *TCSP Guidance*, 2019, link.

[335] FATF, *TCSP Guidance*, 2019, paragraph 198, link.

[336] Egmont-FATF Joint Report, *Concealment of Beneficial Ownership,* 2018, paragraph 5, link.

[337] OECD, *Global Forum on Transparency and Exchange of Information for Tax Purposes: Luxembourg 2019 (Second Round)*, 2019, paragraph 61, link.

[338] While the term of "nominee investor" is used by some professionals in the collective investment sector, the more adequate terminology would be "intermediated position"/ "intermediaries"/ "omnibus accounts"/"segregated accounts", in line with/as detailed in the FATF RBA Guidance on the Securities Sector published in October 2018. To be noted that the main rationale for using such intermediaries in the collective investments sector is twofold. First, the dilution of transaction fees and second, to grant a larger access to investment products for retail investors. Moreover, professionals must assess the quality of the AML/CFT framework of the "intermediary" and the latter must in turn apply adequate due diligence on the investor. In addition, specific enhanced mitigation measures on cross-border intermediaries' relationships are applied by CSSF supervised Luxembourg investment funds or their delegates. Thus, the use of "intermediaries" is a common practice to enable economies of scale within the retail sub-sector.

[339] Egmont-FATF Joint Report, *Concealment of Beneficial Ownership,* 2018, link.

[340] MoJ, *Legal persons and legal arrangements ML/TF vertical risk assessment*, 2022, link.

Grand-Duchy of Luxembourg. For the legal arrangements that have a *fiduciaire* or a trustee registered in an EU Member State, they must provide the AED with an equivalent registration certificate or an extract of the BO information kept in a comparable registry.

In order to make sure that the RFT's information is up-to-date, the 2020 RFT Law foresees that the professionals and persons who have access to the registry shall report any discrepancies found between the data in the RFT and the information in their own records to the AED.

The RFT went live during the second half of 2020. By 31 December 2024, 4 838 trusts and *fiducies* (out of which 2 894 were active at that date) had registered their BO information[341]. As stated in section 6.5.2, 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.

Pursuant to the 2020 RFT Law, the AED has the power to order *fiduciaries* and trustees to register or update their information. The relevant supervisory authority or SRB can monitor whether the professionals acting as a trustee or *fiduciaire* are accurately reporting to the RFT. The AED has the capacity to refuse a registration when it is not complete or accurate and the trustee or *fiduciaire* has up to 15 days to update the information. Additionally, the AED can monitor the compliance by accessing any document related to the *fiducie* or express trust and by requesting information from the supervisory authorities or SRBs. The AED can also instruct the trustee or *fiduciaire* to update the information held with registry or to provide accurate information. When failing to do so, the AED can impose a fine of up to EUR 25 000 for non-compliance (article 21 of the 2020 RFT Law).

As analysed in the 2022 LPs/LAs VRA[342], the information gathered by the RFT shows that TCSPs offering trust services are mostly legal persons, with the remainder being natural persons (17,5% as of end 2023[343]). Additionally, there is a high concentration of legal arrangements managed by TCSPs. Most of these TCSPs are either FIs supervised by the CSSF or professionals controlled by an SRB. Either way, these actors (i.e. trustees and fiduciaries) must apply robust AML/CFT measures. Consequently, these safeguards suggest that the information registered with the RFT is reliable.

**Insight Box 20: Regulated securitisation vehicles supervised by CSSF**

Regulated securitisation vehicles are securitisation undertakings governed by the Law of 22 March 2004 on securitisation that issue financial instruments to the public on a continuous basis (more than three issues per year) and are then supervised by the CSSF. They fall within the scope of the 2004 AML/CFT Law when they perform TCSP activity.

End of 2023, Luxembourg counted two CSSF regulated securitisation undertakings acting as a *fiduciaire* in a *fiducie*. AuM of those two regulated securitisation undertakings decreased from EUR 2,4 billion as of 31 December 2020 to EUR 1,6 billion as of 31 December 2023 (with a peak AuM amounting to EUR

[341] AED.

[342] MoJ, *Legal persons and legal arrangements ML/TF vertical risk assessment*, 2022, section 4.4.3.2, link.

[343] Updated data from AED.

3,5 billion in 2021). The market leader accounted for 98% of market share in 2023. Ownership of these regulated securitisation undertakings was 100% international, but from European countries (Dutch and Swiss).

Products were mainly distributed in the EU and the European Free Trade Association (EFTA), but some products were also distributed in Asian markets. Targeted investors were retail and institutional investors and all regulated securitisation vehicles had a Luxembourgish banking institution providing custody for liquid assets and securities, which ensured indirect AML/CFT supervision.

### *6.6.2. Cash*

Overall, cash (or euro banknotes) can be (i) used for transactional purposes, (ii) stored domestically and (iii) demanded outside the euro area for both transactional and store of value purposes[344]. In spite of a steady growth in non-cash payments and a moderate decline in the use of cash for payments, the total value of euro banknotes in circulation worldwide continues to rise year-on-year beyond the rate of inflation within the Eurozone. This trend is referred to as "the paradox of banknotes": the demand for euro banknotes has constantly increased while the use of banknotes for retail transactions seems to have decreased. According to the European Central Bank (ECB), this seemingly counterintuitive paradox can be explained by demand for banknotes as a store of value in the euro area (e.g. euro area citizens holding cash savings) coupled with demand for euro banknotes outside the euro area[345].

Generally, typologies related to cash as identified in the 2020 NRA remained relevant. It is, however, to be noted that the ML risks linked to counterfeiting currency is at an historically low level. The total number of counterfeit banknotes withdrawn from circulation was 467 000, which means only 16 counterfeits were detected in one year per 1 million genuine banknotes in circulation in 2023[346]. In line with the above, Luxembourg ML threats stemming from counterfeiting currency are assessed as "Low" (see section 5).

#### *6.6.2.1. High value banknotes (store of value)*

As shown in the table below, the net issuance in the Eurozone was abnormally high during 2020. The COVID-19 pandemic intensified the euro area demand for cash for precautionary purposes (i.e., as a store of value), whereas the transactional demand seems to have further decreased[347]. In 2023, net issuance of euro notes has decreased both in Luxembourg and the Eurozone.

[344] Alejandro Zamora-Pérez, *The paradox of banknotes : understanding the demand for cash beyond transactional use,* 2021, link.

[345] 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.

[346] ECB, *Annual report 2023*, link.

[347] Alejandro Zamora-Pérez, *The paradox of banknotes : understanding the demand for cash beyond transactional use,* 2021, link.

**Table 30: Annual issuance of euro notes in Luxembourg (LU) and other Eurozone countries**

| | | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|---|---|---|
| **Δ Net issuance (values)[348]** | **Δ LU (in EUR billion)** | +1 | +0,7 | +0,36 | +0,17 | -0,1 | -0,1 |
| | **Δ Eurozone (in EUR billion)** | +60,4 | +61,6 | +141,8 | +109,9 | +27,6 | -4,8 |

The BCL noted in its 2020 and 2021 annual reports that demand at euro area for high-value bank notes has increased considerably, especially with regard to the EUR 200 banknote. More precisely, demand for EUR 200 banknotes increased by 34% in the Eurozone in 2021. Nonetheless, this demand has decreased slightly since (-2,3% in 2022 in comparison to 2021 and -1% in 2023 in comparison to 2022). Although no longer issued since the end of 2018[349], the EUR 500 banknote accounted for a significant proportion of the value of all banknotes in circulation in the Eurozone (14,1% in 2020 and 8,5% in 2023) throughout the observation period of this report. In a similar vein, and as noted above, the circulation of the EUR 200 banknote has increased and is supposed to replace the EUR 500 banknote[350,351]. Considering the above, it is assumed that a significant amount of cash is being hoarded.

In this context it should be noted that the Study on the payment attitudes of consumers in the euro area (SPACE) of 2024 reports that 43% of the Luxembourg surveyed individuals keep extra cash reserves. This is slightly above the euro area average (35%)[352].

In this context, it should also be noted that according to the SPACE of 2024, Luxembourg residents had the highest amount of cash in their wallet (median of EUR 82) among the surveyed individuals. Nonetheless, it should be noted that this amount has decreased as well, as SPACE of 2022 reported that Luxembourg surveyed individuals reported more than EUR 110 cash in their wallets.

Importantly, SPACE of 2024 also indicates that 69% of the surveyed Luxembourg residents reported that cards or other cashless payments are their preferred payment instrument whereas 13% indicated having a preference for cash, the lowest percentage in the Euro zone after Finland.

The SPACE of 2024 observed that cash payments are most of the times made in case of low-value transactions. More than 60% of payments below EUR 5 were made in cash while only 27% of transactions above EUR 100 were paid in cash in the Eurozone in 2021[353].

[348] BCL, *Rapport Annuel,* 2018-2021, link with Δ being the difference of net issuance of year N and the net issuance of year N-1.
[349] ECB, ECB ends production and issuance of €500 banknote (press article: May 4, 2016), link.
[350] 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.
[351] BCL, *Rapport Annuel,* 2021, link.
[352] ECB, *Study on the payment attitudes of consumers in the euro area (SPACE) – 2024*, link. Note that surveys with Luxembourg individuals took place in the second half of 2023 and the first half of 2024.
[353] ECB, *Study on the payment attitudes of consumers in the euro area (SPACE) – 2024*, link.

Concerning high denomination banknotes, the 2022 SNRA concludes that related ML risks were "Very high"[354] (cf. section 6.6.2.4). The 2022 SNRA notes that perpetrators could misuse these banknotes to make cash transportation easier as the larger the denominations, the more funds can be shrunk to take up less space. In addition, the 2020 SNRA describes a scenario where counterfeit euro banknotes are sold via online platforms. Although not in relation with counterfeit currency, the following case study describes how individuals may try to abuse even central bank services to introduce banknotes of illicit origine into circulation.

**Case study 15: Reimbursement of damaged banknotes[355]**

In 2019 a first person handed in 15 damaged €200 banknotes to the BCL public counter for reimbursement (EUR 3 000). Then in 2020, a second person first handed in 2 damaged €200 banknotes, and a few days later deposited 24 €100 banknotes and 11 €200 banknotes. This second person's total deposit amounted to EUR 5 000.

In accordance with BCL's procedures for AML and for banknote exchange or refund requests, the two depositors were asked to provide explanations as to the economic origin of the funds and the circumstances that had damaged the notes. After several tedious exchanges with the depositors, the explanations given by the two depositors as to the economic origin and causes of the deterioration of the notes remained unconvincing. In particular, the damage to the deposited banknotes raised serious doubts. These suggested that all the banknotes deposited were linked to the case of the so-called "Libyan" banknotes stolen by terrorist groups from the foreign exchange reserves of the Central Bank of Libya. This suspicion was confirmed by an analysis of the notes. Both cases were reported to the CRF and to the State Prosecutor.

In 2024, the depositors were convicted of money laundering, one to a six-month suspended prison sentence and a fine of EUR 4 000, sentences upheld on appeal, and the second to a fine of EUR 2 500. The courts ordered the definitive confiscation of the banknotes seized.

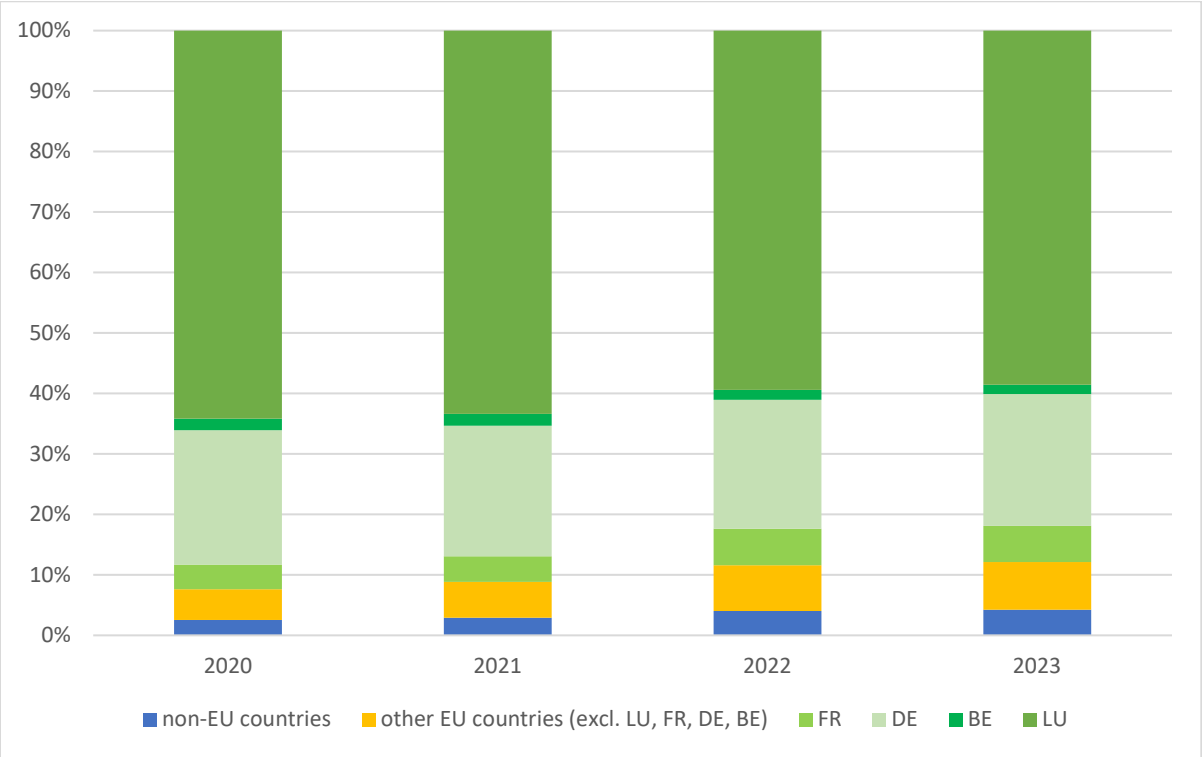
#### *6.6.2.2. Payments in cash (transactional)*

Data from the BCL on the value and location of ATM withdrawals from Luxembourg accounts suggests that the total value of ATM withdrawals performed has increased between 2020 and 2023. Whereas the total value of ATM withdrawals reached EUR 3,355 billion in 2020, withdrawn amounts on ATMs rose by 14% in 2023, reaching EUR 3,821 billion. As depicted in the graph below, the majority of withdrawals were performed on machines located in Luxembourg (60%). Withdrawals from other European countries remained considerable (about 35%). Furthermore, withdrawals in non-EU countries accounted for the least significant share (about 5%), although this proportion has slightly increased during the observation period of this report.

[354] 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.

[355] Case study provided by the BCL.

**Figure 28: Location of ATM withdrawals from Luxembourg accounts (value of withdrawals), 2020 – 2023, BCL data**




Taking a closer look at the geographic distribution of ATM withdrawals performed in EU and non-EU countries, it seems that withdrawals occurring in foreign countries remain quite concentrated around Luxembourg's neighbouring countries. Other relevant EU countries are for instance Portugal, Austria, Italy and Spain (among the 7% of total ATM withdrawals in "other EU countries", these countries accounted for 80% of these withdrawals in 2023). Withdrawals in non-EU countries occurred predominantly in the UK, Switzerland, and Türkiye. Nonetheless, fragmentation within this category was higher as these 3 countries represented 22% of total withdrawals within this category in 2023.

Overall it seems that the geographical distribution of these ATM withdrawals is in line with Luxembourg's geographical context, demographic structure (see section 3) and Luxembourg's residents frequented travel (leisure and business) countries[356].

#### *6.6.2.3. Cash-intensive businesses*

The 2022 SNRA notes that cash-intensive businesses may be abused by criminals to launder large amounts of cash that are proceeds of crime by justifying its origin from (fictitious) economic activities[357].

[356] STATEC, *Tourisme en chiffres – édition 2024*, link.

[357] 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.

Globally, money remittance providers, dealers in goods and casinos have, amongst others, traditionally been exposed to ML risks associated with cash due to specific characteristics of the sector (e.g. being cash-intensive).

Casinos and other entities associated with gambling are typically also cash-intensive, often operating 24 hours per day with high volumes of large cash transactions taking place very quickly. However, in Luxembourg there is only one casino (operating from 10 am to 3 am, respectively 4 am during the weekend) and other gambling activities are deemed low risk (cf. section 6.3.4).

As noted under section 6.3.3, key risks with regard to product and services by these professionals is the cash usage in the sector (although it should be noted that it has generally declined, see for instance Insight Box 13).

**Case study 16: Cash payment**

The case started with a traffic offence committed by the driver of a luxurious Italian car. During the preliminary investigation, the State Prosecutor found out that the car had been acquired and paid for by a French company, whose BO was the driver's wife. The suspicion of abuse of company assets was referred to the French authorities and to the AED. In this respect, the AED carried out an in-depth inspection of the car dealership and discovered suspect cash transactions, which it reported back to the State Prosecutor.

Based on the AED's findings, the State Prosecutor opened a preliminary investigation against the car dealership. It came out that the car had been purchased, in July 2014, by a local businessman for EUR 49 500. In order to negotiate a better price (EUR 48 000), the businessman paid EUR 48 000 in cash. Despite the fact that the amount of EUR 48 000 was paid in a single instalment, it was recorded in the cash book as five successive payments of amounts ranging from EUR 8 000 to EUR 10 000, each below the threshold defined by the 2004 AML/CFT Law.

When interviewed, the managing director explained that the employees of the car dealership had not received any AML/CFT training but were only given documentation from the Chamber of Commerce on the fight against ML. The managing director further admitted that there were no internal AML/CFT procedures in place. He explained that his father accepted the EUR 48 000 in cash and presented him with the *fait accompli*. He acknowledged that, at the time of the facts, he was the sole managing director of the car dealership. The statements made by the defendant also showed that the car dealership no longer accepted cash payments exceeding EUR 15 000 and that customers making cash payments must provide a proof of their identity.

Both the legal entity operating the car dealership and the managing director were convicted by the District Court for misdemeanour matters. The legal entity was sentenced to a fine of EUR 5 000 and its director to a fine of EUR 2 500. As the AED had already applied an administrative sanction, the District Court declared that, in this specific context, the principle of *non bis in idem* did not apply, leading to the conclusion that criminal and administrative sanctions can coexist. The decision is final.

#### *6.6.2.4. Cash couriers*

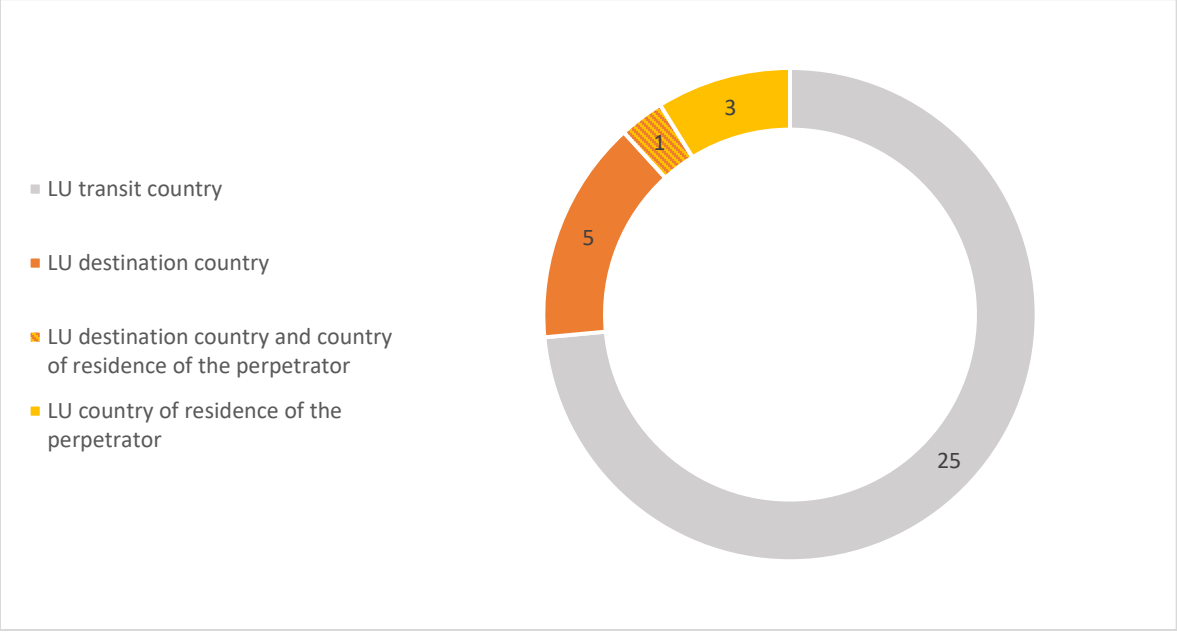
As noted in the 2022 SNRA, criminals who generated cash proceeds usually seek to aggregate and move these ill-gotten gains from their source by either repatriating or moving them to locations where access to placement is easier. Cash can be transported by a courier (i.e. "accompanied" cash) or by a post parcel service (i.e. "unaccompanied" cash). Overall, the physical transportation of cash is estimated to be one of the oldest and most basic forms of ML.

As noted above, high value bank notes make cash transportation easier as the larger the denominations, the more funds can be shrunk to take up less space. Couriers may use road, rail or air transport to move those funds cross-border. In addition, criminals may use sophisticated concealment methods of cash (for example, cash that is hidden within goods).

The 2022 SNRA further notes that cash smuggling may occur at other stages and is also used by non-cash generating offences. For example, CEF make use of money mules to receive and withdraw sums fraudulently obtained from victims' bank accounts in cash (cf. see section 5). These funds are thereafter sent via wire transfer to other jurisdictions where they are collected in cash by a select number of individuals, likely for onward transportation. Nevertheless, the 2022 SNRA concludes that drug trafficking is supposed to be the most relevant crime area with regard to illicit cash movements.

During the observation period, the ADA detected 34 infringements in the context of its cash controls. Considering the limited size of the country and its geographical position (i.e., in the middle of Europe), detected cash flows were most of the times in transit (25 cases).

**Figure 29: Nature of cash flows in the context of infringements established by ADA, 2020 - 2023**




All Member States of the EU reported over 8 700 infringements with respect to cash declarations between June 2023 and June 2024, respectively over 8 100 between June 2022 and June 2023. Associated values amount to EUR 199 000 and EUR 220 450 000 respectively. Taking into consideration the number and the

amounts related to infractions to the law on entering and leaving the EU, it seems that the average amount of cash related to infringements was situated between EUR 20 000 and EUR 30 000 in these two years[358]. In Luxembourg, the average amount of ADA interceptions amounted to EUR 34 000 in 2023.

## 6.7. Emerging and evolving vulnerabilities

### *6.7.1. Crowdfunding*

Crowdfunding is an alternative form of financing that connects those who can give, lend or invest money directly with those who need financing for a specific project. It usually refers to public online calls to contribute to the financing of specific projects. Several crowdfunding models have emerged within the EU over the past couple of years, such as the donation-based, lending-based, investment-based, or reward-based crowdfunding[359].

The vast majority of crowdfunding activities is legitimate and a licit way of gathering funds from masses of people. However, it has been globally observed that these platforms could be exposed to ML risks.

According to the 2022 SNRA, ML risks linked to crowdfunding activities varied in accordance with the models employed by the platforms. For instance, crowdfunding platforms focusing on activities that collect funds for later onward transmission (and are thus stored on the investor's account) are particularly vulnerable for ML abuse. Lending and securities platforms are considered to have a higher inherent risk than donations platforms, as they allow to raise larger amounts[360].

The 2022 SNRA further indicates that the risks with regard to crowdfunding platforms rise if those platforms allow the use of virtual currencies or (anonymous) electronic money. Furthermore, risks may also vary depending on whether the platform is directly linked to a FI or left to private initiatives on the web. In this case, they would fall out of the scope of the AML/CFT framework. The complexity linked to crowdfunding services (cross-border nature of transactions, number of people and intermediaries involved) further increases ML risks.

The European Commission adopted Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European Crowdfunding Service Providers for business and, since 10 November 2021, the provision of investment and lending-based crowdfunding services from Luxembourg is subject to the procurement of a license as a European Crowdfunding Service Provider (ECSP), which thus entails falling under the prudential supervision of the CSSF. This regulation requires all payments to be carried through an authorised Payment Service Provider (PSP) and introduces other safeguards to mitigate some of the risks. Nevertheless, this regulation does not apply to all crowdfunding models. Donation- or reward-based platforms do not fall under the above-mentioned regulation. Furthermore,

[358] Cash Controls Statistical Data 3 June 2022-2 June 2023 (inclusive) according to Article 18 of Regulation (EU) 2018/1672 on controls on cash entering or leaving the Union, link and Cash Controls Statistical Data 3 June 2023-2 June 2024 (inclusive) according to Article 18 of Regulation (EU) 2018/1672 on controls on cash entering or leaving the Union, link.

[359] CSSF, Crowdfunding service providers, link.

[360] 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

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. In Luxembourg, no entity has been granted a license as an ECSP yet. Should an ECSP intend to provide payment services in addition to the crowdfunding services, a separate licence under the Law of 10 November 2009 on payment services may be required[361].

In Luxembourg, the most significant ML risks with regard to crowdfunding platforms stem from financial services offered to global crowdfunding platforms. While the overall crowdfunding market in Luxembourg is considerable (the market volume has been estimated at between USD 10 million and USD 100 million in 2019[362]), a significant part of global crowdfunding uses payment methods such as bank transfers, credit and debit cards, and internet payment services[363]. Luxembourg banks, PIs and EMIs offer such services to other professionals abroad. However, only one bank was offering this service as of 31 December 2023[364], as was also one MVTS provider (which concerned only very few platforms). In this context, it is also important to note that this latter professional reviewed its strategy and has dwindled its client-base in order to focus on "high-quality platforms".

### *6.7.2. Hawala and other service providers*

Although there is no evidence that hawala and other similar service providers (HOSSPs) operate in Luxembourg, the following section describes and illustrates the purpose and function of these providers.

Hawala payments are informal funds' transfers that are made without the involvement of authorised FIs. In principle, the money does not physically move from the payer to the payee. Instead, as is also often the case for money remittances, the transfer is done by offsetting balances between the hawaladar (those that operate hawala) of the payer and the hawaladar of the payee. The term HOSSPs is often used to describe a number of different informal value transfer systems which have similar properties and operate in similar ways, although they are not strictly hawala.

**Insight Box 21: Hawala – illustration**

A hawaladar from country A (HA) receives funds in one value (cryptocurrency, gold, goods, etc.) from the payer and, in return, gives the payer a code for authentication purposes. He then instructs his counterpart in country B (HB) to deliver an equivalent amount in the local currency to a designated beneficiary, who must disclose the code to receive the funds. After the remittance, HA has a liability to HB, and the settlement of their positions is made by various means, either financial or goods and services.

HOSSPs are not only cheaper (with margins as low as 1% for international transfers), but also quicker than transactions in the regular financial system. In addition, customers do not need to prove their identity or

[361] CSSF, Crowdfunding service providers, link.

[362] Cambridge Centre for Alternative Finance, *The 2nd Global Alternative Finance Market Benchmark report*, 2021.

[363] Asia/Pacific Group on Money Laundering and Middle East and North Africa FATF (MENAFATF), *Social Media and Terrorist Financing*, 2019.

[364] Information provided by the CSSF.

give reasons for why the money is being sent. This explains why it is essential in countries where large parts of the population do not have identity documents. In countries where access to basic financial services (such as a bank account) is limited, HOSSPs often enable people to send or receive legitimate remittances.

At the same time, the implementation of stricter AML/CFT regulations in mainstream FIs has also made informal value transfer systems and HOSSPs increasingly attractive to organised crime groups, who frequently use them to transfer illegitimate remittances, i.e. transfer large amounts of criminal proceeds or to launder such criminal proceeds, providing layering and remittance services. The opacity provided by HOSSPs is another key risk driver with regard to ML. As there are no direct money/value flows between sender and receiver, tracing the money/value flow is a challenge.

## 6.8. Unintended consequences resulting from the FATF standards and its implementation: de-risking and financial exclusion

De-risking is the phenomenon of FIs terminating or restricting business relationships with clients or categories of clients in order to avoid, rather than to manage, their risks in line with a risk-based approach. In this respect, it is important to highlight that de-risking is, by definition, inconsistent with a proper application of the risk-based approach. Consequently, de-banking, or the loss of any financial services, may or may not constitute de-risking depending on the reasons for it[365]. The phenomenon of de-risking has been observed in many jurisdictions, especially in those where compliance with international AML/CFT standards is high. Overall, it is quite challenging to strike the right balance between financial inclusion and the ever-growing AML/CFT requirements.

Unwarranted de-risking is a significant issue across the EU, with a potential adverse impact on its financial system's stability and integrity. Furthermore, impacted customers may resort to alternative, unregulated payment channels (e.g. HOSSP, see section 6.7.2) to meet their financial needs. Consequently, transactions may no longer be subject to monitoring, which makes detection and the reporting of suspicious transactions difficult. Ultimately, this may have an adverse impact on the prevention of ML[366].

The Law of 13 June 2017 on payment accounts (2017 Law on payment accounts) grants natural persons residing in the EU access to a payment account with basic features. The CSSF has highlighted via different communication channels the obligation applicable to several Luxembourg FIs to provide consumers with payment accounts with basic features. The names of these FIs are publicly available on its website[367]. This right extends to natural persons who do not dispose of a residence permit but whose expulsion is impossible and who are not acting for business purposes. In this respect, it is also important to note that all types of social benefits and aids (e.g. social benefits, unemployment benefits) from the Luxembourg State are sent to natural persons via bank transfer. In 2017, the World Bank reported that 99% of Luxembourg's adult population held a bank account[368]. Consequently, financial inclusion with respect to

[365] FATF, *High-Level Synopsis of the Stocktake of the Unintended Consequences of the FATF Standards,* 2021, link.
[366] EBA, *Consumer trends report,* 2024/25, link.
[367] CSSF, Basic payment account/payment account with basic features, link.
[368] World Bank, Global Findex Database, 2017, link.

natural persons is assessed to be very high in Luxembourg. De-risking therefore impacts Luxembourg natural persons to a lesser extent.

Whereas natural persons in Luxembourg are less affected by the consequences from de-risking, Luxembourg identified different categories of legal persons that may be impacted by de-risking:

- Entrepreneurs residing in Luxembourg that emigrated from countries with weak AML/CFT frameworks;
- Due to the complexity of their business model and transactions, entities active in VAs, FinTechs and Start-ups;
- SMEs that are active in higher risk sectors (e.g. the legal CBD market) or maintain business with higher risk countries;
- Some private equity structures; and
- NPOs active in jurisdictions with a weak AML/CFT framework or with an active terrorist threat.

The EBA identified three main key drivers of de-risking. These drivers are not mutually exclusive and, in practice, are very often combined[369]:

- ML/TF risks exceed institutions' ML/TF risk appetite: Over the last decades, AML/CFT requirements have become more and more complex and stringent. FIs risk severe penalties for any detected AML/CFT shortcomings by the relevant supervisor. Consequently, ML/TF risk appetite has decreased for many institutions considering the legal, financial and reputational risks;
- Lack of expertise by institutions in specific customers' business models: Some institutions lack the expertise necessary to understand the way NPOs operate (i.e., a model based on trustees and beneficiaries located in multiple jurisdictions, etc.), or do not have requisite knowledge to deal with entities active in VA or FinTech firms; and/or
- Cost of compliance: For instance, dealing with customers with links to jurisdictions presenting higher ML/TF risks will entail enhanced due diligence in the monitoring of cross-border transactions, including enhanced scrutiny of customers' relationships and their network of transactions.

Considering the challenges faced by these types of legal persons (e.g. SME, FinTech firms, Start-ups), the ABBL, the Luxembourg Chamber of Commerce and the House of Entrepreneurship published a guide in English, French and German in order to help entrepreneurs open and maintain a bank account[370].

The publication of this general guidance document was followed by the publication of specific guides to the attention of particular segments of clients, starting with *Sociétés commerciales*[371] and *ASBLs*[372]. Additional publications will follow in the coming months so as to cover other segments, such as trusts, *Fondations* and investment funds.

[369] European Banking Authority, *Opinion of the European Banking Authority on de-risking*, 2022, link.
[370] ABBL, Open a professional bank account, link.
[371] ABBL, Commercial businesses: Your path to a successful bank account opening, link.
[372] ABBL, Non-profit associations: Opening a bank account for non-profit associations, link.

In addition, the ABBL has approached its members to compile a list of dedicated contact persons within banks and other providers of banking services in Luxembourg potentially interested in onboarding particular segments of corporate clients. Relevant listings are publicly available on the ABBL website and are updated on a regular basis[373]. These publications are part of a broader effort of the ABBL and its members to make the opening of a bank account and access to banking services as simple and transparent as possible.

Furthermore, within the working groups of the NPC, public and private actors engaged in outreach sessions and activities in order to bridge the needs of those concerned with the requirements of the FIs. This helped raise awareness of the challenges encountered by both sides and to collectively find ways on how to remedy, to the extent possible, the phenomenon of de-risking.

[373] ABBL, Bank account opening: dedicated contacts for AIFs, FinTechs and SMEs, link.

# 7. Mitigating factors assessment

Luxembourg's AML/CFT regime is based on a solid legal framework consistent with the FATF recommendations and the 4th and 5th EU AML/CFT directives. A comprehensive institutional set-up, involving a wide range of competent authorities to prevent, supervise, detect, investigate and prosecute ML/TF and to recover related assets, is in place and is recognised as delivering good results, as evidenced by the FATF 4th round mutual evaluation of Luxembourg. The national AML/CFT framework effectively mitigates the inherent risks detailed in the previous sections, as reflected in the resulting residual risk.

Luxembourg's national strategy encompasses both ML and TF and is informed by the NRAs and the SNRAs. The first NRA was adopted in 2018 by the NPC and updated in 2020, whereas the first SNRA on the risks of ML/TF affecting the internal market was conducted by the European Commission in 2017 and updated in 2019 and 2022. To further enhance its understanding of high-risk sectors, the NPC conducted various VRAs, such as on VASPs, legal persons and legal arrangements and on TF. They are published on the MoJ's website in both English and French[374].

Following a risk-based approach, the CSSF further conducted and published sub-sectoral risk assessments for particular sub-sectors, such as on private banking[375] (published in 2019 and updated in 2023), collective investments[376] (published in 2020, then updated in 2022 and lastly in 2025) and specialised PFSs providing TCSP activities[377] (published in 2020). These risk assessments are freely available on the CSSF's website.

In a similar vein, the CRF disseminated via goAML a number of typology reports and red flag indicators, such as the typology report on the real estate sector, the typology report on the circumvention of financial restrictive measures and the yearly typology report on the investment sector.

Detailed statistics on Luxembourg's AML/CFT measures were also consolidated on the MoJ's website.

## 7.1. National coordination and the AML/CFT strategy

The Grand-Ducal Decree of 10 November 2021 established the Inter-ministerial Steering Committee for the Fight against Money Laundering and Terrorist Financing (ISC). 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.

The ISC 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.

[374] MoJ's webpage, link

[375] CSSF, *ML/TF Sub-Sector Risk Assessment - Private Banking (2023 update)*, link.

[376] CSSF, *ML/TF Sub-Sector Risk Assessment - Collective Investment Sector (2025 update),* link.

[377] CSSF, *ML/TF Sub-Sector Risk Assessment - Specialised Professionals of the Financial Sector providing Corporate Services (Trust and Company Service Provider activities)*, link.

The ISC elaborated the 2023-2024 AML/CFT strategy. It was adopted by the Government Council in October 2022 and consisted of the following four priorities:

- **Priority 1:** Ensure reliable information on the transparency of legal persons, including non-profit organisations, and legal arrangements, and monitor the evolution of ML/TF typologies in this area;
- **Priority 2:** Optimise the supervision and enforcement through efficient allocation of resources using the risk-based approach;
- **Priority 3:** Strengthen the operational capacity and effectiveness of the authorities responsible for the detection, investigation, prosecution of economic and financial crime and asset recovery and management; and
- **Priority 4:** Mitigate the ML/TF risks associated with new technologies and support the digital transformation of AML/CFT authorities.

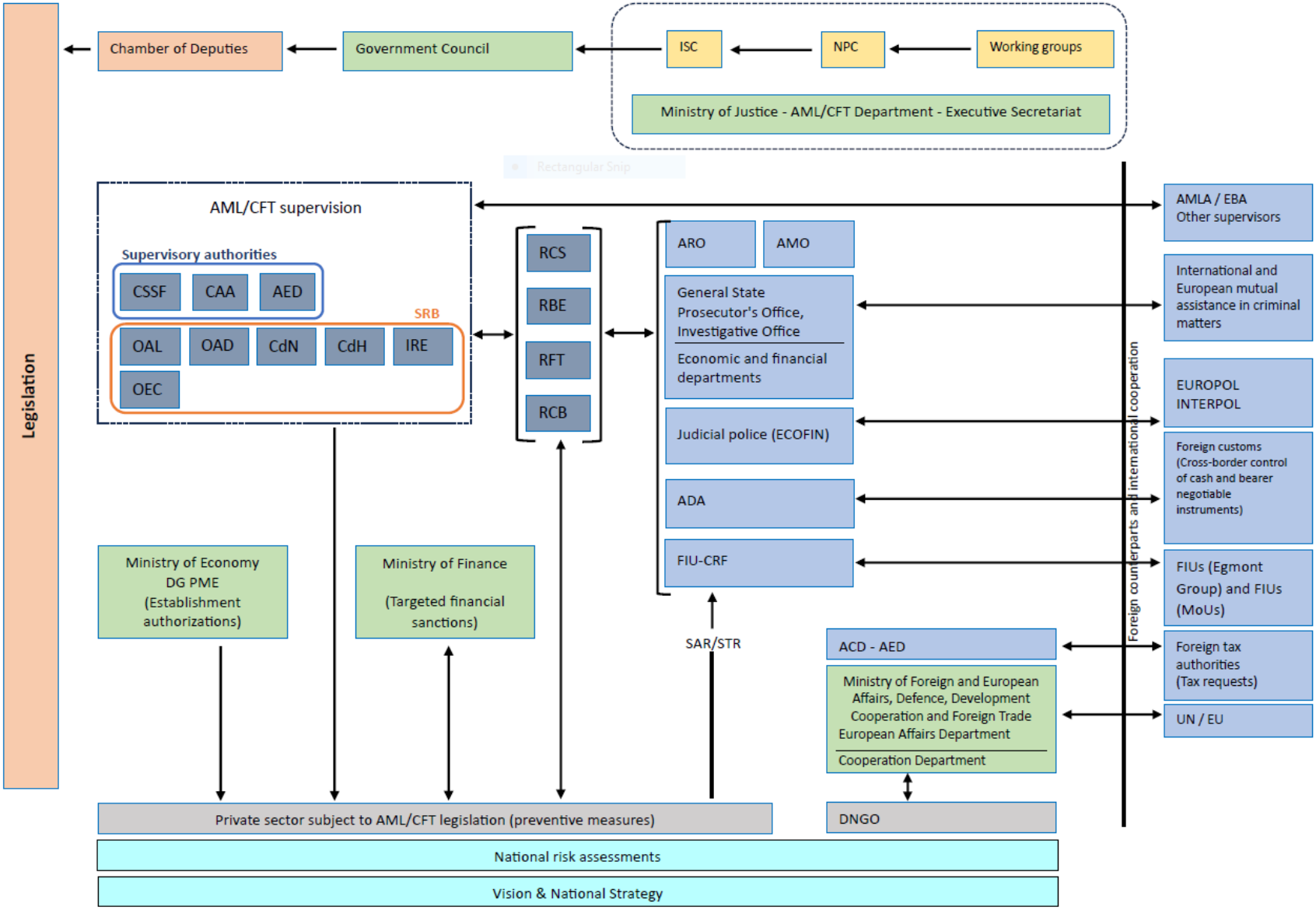
The NPC is chaired by the national AML/CFT coordinator and is composed of operational members, such as representatives of the supervisory authorities (CSSF, CAA and AED), SRBs (OAL, OAD, CdN, CdH, IRE and OEC), the CRF, the investigation and prosecution authorities and of the private sector. The high-level 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.

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.

The following chart provides an overview of Luxembourg's national coordination set up:

**Figure 30: Luxembourg's national coordination set up**



## 7.2. National cooperation

National coordination and cooperation on AML/CFT issues is a recognised strength of Luxembourg AML/CFT system[378].

At a strategic level, article 9-1 of the 2004 AML/CFT Law provides for the strategic cooperation between the members of the NPC (see section above).

At an operational level, article 9-1 of the 2004 AML/CFT Law provides for the cooperation between the CRF and the supervisors. The supervisory authorities and the SRBs cooperate closely with the CRF and amongst themselves. They are authorised to exchange information that is necessary for the fulfilment of their respective duties within the framework of the fight against ML and TF.

Additionally, articles 74-2 and 74-4 of the 1980 Judiciary Organisation Law provide for close cooperation between the CRF and competent AML/CFT stakeholders.

Moreover, article 16 of the modified 2008 Tax Authorities Cooperation Law foresees the cooperation between judicial authorities and the CRF on the one hand, and the AED and ACD on the other hand.

The Code of Criminal Procedure foresees cooperation mechanisms between judicial and investigative authorities.

In the field, this cooperation between AML/CFT actors at the national level is facilitated by a series of MoUs, the participation in each other's technical committees and the establishment of expert group meetings in specific areas.

## 7.3. Prevention and supervision: supervisory authorities, SRBs and other relevant authorities

Luxembourg supervisors continue to ensure that the private sector effectively implements its AML/CFT obligations by following a risk-based approach.

Luxembourg counts three supervisory authorities (CSSF, CAA and AED) and six SRBs (OAL, OAD, CdN, CdH, IRE and OEC) in charge of AML/CFT supervision covering the different types of professions falling within the scope of the 2004 AML/CFT Law.

Through regular training of their AML/CFT staff, participation in (inter)national working groups and outreach activities with the private sector, supervisors have a good understanding of ML risks in their supervised sectors. This understanding leverages the implementation of the risk-based approach within their supervisory activities. Usually, those encompass both off-site supervisory measures and on-site inspections. Identified deficiencies are subject to follow-up actions and breaches are subject to enforcement measures.

[378] FATF, *Anti-money laundering and counter-terrorist financing measures. Luxembourg. Mutual Evaluation Report*, 2023, link.

**Case study 17: Improvement of Compliance culture**[379]

Following an on-site inspection, a professional was enjoined to remediate several deficiencies by i.a. conducting regular reviews of clients' risk ratings and KYC files including tax aspects.

The professional started a remediation plan and attended a face-to-face meeting with the CSSF. As the professional was not on track with the remediation plan due to a lack of resources, the CSSF decided to closely follow-up on this matter and meet the professional every quarter. In parallel, an on-site inspection started on a related subject and led to an administrative fine. The professional realized that its Compliance culture had to be improved. The professional increased its resources dedicated to the KYC remediation plan, reorganised its Compliance function and hired additional experienced persons. At the end of the remediation plan, several members of the team joined the professional.

In addition to the strong preventive and supervisory actions performed by the supervisors, market entry controls add an additional layer to Luxembourg's AML/CFT framework, as evidenced in case study below.

**Case study 18: Individual implicated in various money laundering scandals discouraged from taking over a bank**[380]

In 2022, the CSSF was informed that the owner of a bank under its supervision had negotiated, subject to regulatory approval, the sale of his majority stake to an individual as reference shareholder. Preliminary research completed by the CSSF revealed that the said individual was implicated in various ML scandals during his prior roles in other European countries. Suspicions regarding his suitability were reinforced through consultations with the CRF and the supervisory authorities of the two countries concerned.

CSSF successfully prevented the proposed acquirer from taking a stake in the bank.

### *7.3.1. Financial sector supervisory authorities*

The CSSF ensures the prudential and the AML/CFT supervision of Luxembourg's financial sector. The CAA is in charge of the prudential and the AML/CFT supervision of Luxembourg's insurance sector.

In March 2020, during the observation period of this NRA update, Luxembourg created a central electronic data retrieval system related to IBAN accounts and safe-deposit boxes held by credit institutions in Luxembourg (amended Law of 25 March 2020 establishing a central electronic data retrieval system related to IBAN accounts and safe-deposit boxes). This central register is a key mitigating factor allowing to perform searches and investigations on the holders of IBAN accounts or safes in Luxembourg. Several authorities, such as the CRF and the Asset Recovery Office (ARO), have direct access to the register, whereas other national authorities and SRBs have an indirect access via the CSSF, which is the current manager of the central register.

[379] Case study provided by the CSSF.

[380] Case study provided by the CSSF.

**Insight Box 22: Central register of bank accounts**

The Directive 2024/1640 (AMLD6) of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849 (AMLD6) foresees that centralised automated mechanisms (in Luxembourg, currently the central register of bank accounts) shall include information on bank accounts, including vIBANs, and payment accounts, securities accounts, crypto-asset accounts and safe deposit boxes, and those centralised automated mechanisms shall be interconnected at EU level, to enable Financial Intelligence Units "*to obtain swiftly cross-border information on the identity of holders of bank accounts and payment accounts, securities accounts, crypto-asset accounts and safe deposit boxes in other Member States, which would reinforce their ability to effectively carry out financial analysis and cooperate with their counterparts from other Member States".*

This text should be transposed by July 2027 at latest by EU Member States.

As noted previously, the Law of 25 March 2020 amending the 2004 AML/CFT Law added VASPs within the scope of the CSSF AML/CFT supervision.

### *7.3.2. Non-financial sector supervisory authorities and SRBs*

Legal professions, CPA and auditors in Luxembourg are supervised by SRBs for AML/CFT purposes:

- The IRE is in charge of ensuring AML/CFT supervision among (approved) statutory auditors and (approved) audit firms;
- The OEC is in charge of ensuring AML/CFT supervision among CPAs;
- The CdN is in charge of ensuring AML/CFT supervision among notaries;
- The OAL and OAD are in charge of ensuring AML/CFT supervision of lawyers carrying out services subject to the 2004 AML/CFT Law; and
- The CdH is in charge of ensuring AML/CFT supervision of bailiffs.

The AED is Luxembourg's AML/CFT supervisory authority for professionals subject to the 2004 AML/CFT Law but that are not supervised by another supervisory authority or SRB. This includes AML/CFT supervision for REAs and REDs, accountants, some TCSPs, gambling service providers, freeport operators and some dealers in high value goods.

### *7.3.3. Legal persons and legal arrangements*

Mitigating factors to prevent the misuse of legal persons and legal arrangements include licensing, VAT registration and tax controls, the registers (RCS for basic information, RBE and the RFT for BO information), and supervision of obliged entities involved in the creation and maintenance of legal persons and legal arrangements.

Luxembourg follows a multi-pronged approach to obtain accurate, adequate and up-to-date basic and BO information on legal persons through three sources: (i) the registers (RCS and RBE for basic and beneficial

ownership information), (ii) the obliged entities with whom they enter into a business relationship or with whom they have an occasional business relationship and (iii) the legal persons themselves.

The law of 7 August 2023, on non-profit associations and foundations (2023 NPAF Law) has replaced the law of Law of 21 April 1928 on non-profit associations and foundations (1928 NPAF Law). The main ambitions of the 2023 NPAF Law were to:

- increase financial and organizational transparency of associative entities;
- impose an annual filing of accounts to ensure clear and rigorous financial monitoring; and
- implement meticulous record-keeping of members, thus facilitating quick access to information in case of official requests.

Overall, the 2023 NPAF Law seeks to meet international standards, in line with Recommendation 8 of the FATF, and on the other hand, to prevent any misuse of organisations for malicious purposes, such as for ML and for TF.

In line with the provisions set out in the 1915 Companies Law, the 2023 NPAF Law also established a simplified administrative dissolution procedure without liquidation, allowing for efficient updating of data in the RCS, in line with international requirements. Nonetheless, while strengthening transparency, Luxembourg has ensured that the new measures do not hinder the enthusiasm and passion that drive the actors of Luxembourg's non-profit sector.

**Insight Box 23: Launch of website myasbl.lu**

To raise awareness on the modifications stemming from the implementation of the 2023 NPAF Law, the MoJ launched the website https://myasbl.lu/.

This website provides useful information on the raison d'être of this new and revised legal framework, an overview of the main changes and more detailed information on, for example accounting and filing obligations.

The website also includes a dedicated section on ML and TF risks in order to prevent the misuse of NPAF for ML and TF purposes.

Explanatory videos and guidance help to provide the reader with further useful information in order to comply with the new framework.

In this regard, the MoJ has organised and participated in a number of different workshops, conferences and trainings in order to raise awareness about this new legal framework and the potential ML/TF risks with regard to NPOs.

## 7.4. Detection

### *7.4.1. Cellule de renseignement financier*

The *"Cellule de renseignement financier"* (CRF) is the national authority responsible for receiving and analyzing 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[381].

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 March 7, 1980 on the judiciary organisation.

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.

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).

The CRF's analytical function is twofold:

1. The operational analysis which focuses on individual cases and specific targets or on appropriate selected information, depending on the type and volume of information received and the expected use of the information after their dissemination; and
2. 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.

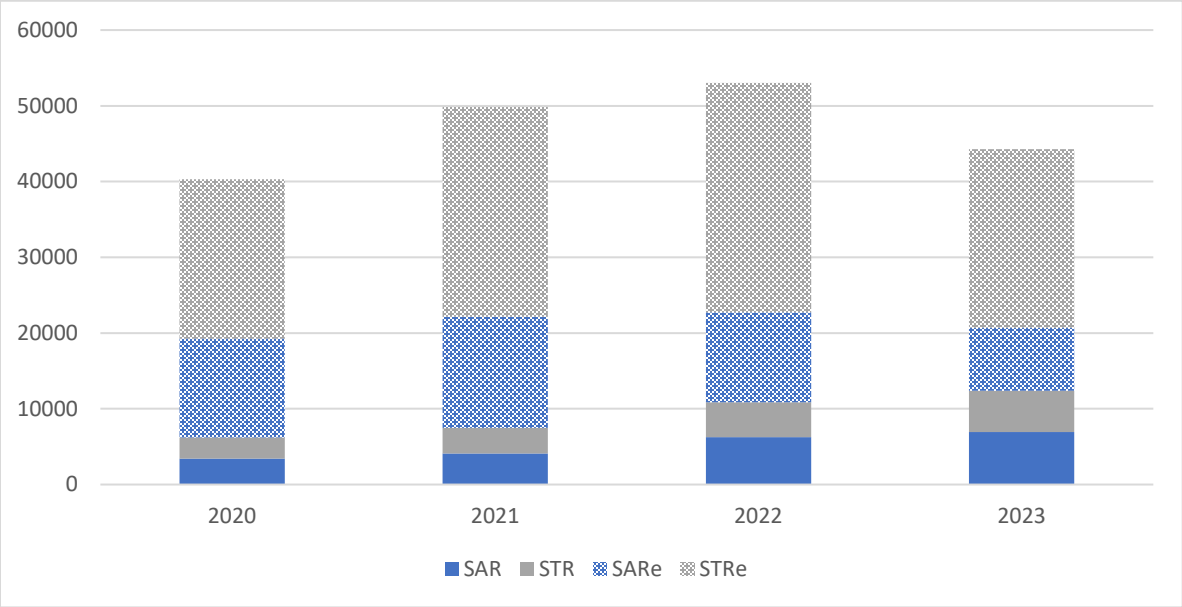
With the amendment of the Law of 16 July 2016 on the organisation of controls on the cross-border transportation of cash (2021 Cash Control Law), magistrates of the CRF have the power to freeze funds upon suspicion (for instance, following receipt of a STR or following cooperation with other FIUs) for 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).

[381] Note that the CRF is under the administrative authority of the General State Prosecutor's Office.

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[382].

The figure below illustrates the number of STRs received during the observation period of this NRA. Overall, the number of filings made by obliged entities remained at an overall high level. Due to the optimisation of filing processes of some entities (especially with regard to electronic STRs/SARs), the number of filings has slightly decreased in 2023 (by around 16%). In this context, it should also be said that filings of "traditional" STR/SAR have almost doubled between 2020 and 2023, with 6 215 STR/SAR in 2020 and 12 395 in 2023.

**Figure 31: Breakdown of ML reports filed by obliged entities with the CRF, 2020 – 2023**




During 2020 and 2023, most reports originated from PIs/EMIs, the banking, the investment and VASP sectors, with most of the reports referring to fraud, counterfeiting and piracy of products and tax crimes as underlying predicate offences. This is in line with the threats and risks assessed earlier in this report.

Compared to the 2020 NRA, the number of STRs received from DNFBPs increased. During the 2020 NRA observation period, the CRF received around 300 STRs from those actors. This number increased continuously to around 500 reports in 2023, with most of them emanating from CPAs. The quality and the volume of these reports continued to increase as well considering the ever-increasing awareness initiatives conducted by supervisors, the CRF and other AML/CFT authorities.

National and international cooperation is essential for Luxembourg's competent authorities. Indeed, one of the core functions of the CRF is the exchange with its (inter)national authorities in AML/CFT matters.

[382] Note that in 2020, 3 049 obliged entities were registered with goAML, 5 048 in 2021, 7 720 in 2022 and 10 417 in 2023. The increase is due to enhanced supervisory actions and awareness raising activities of supervisors and the CRF.

Relevant information held by the CRF is made available to competent authorities and foreign authorities through spontaneous or formal requests for information.

The CRF continues to regularly meet with national AML/CFT authorities to exchange on relevant AML/CFT matters and the reports received. It participates in meetings of the Egmont Group and in multiple national and international fora. To raise awareness on ML/TF matters and typologies among the private sector actors, the CRF also participates extensively in conferences and training sessions. Furthermore, it provides typology reports and strategic analysis products to obliged entities.

### *7.4.2. Administration des douanes et accises*

As noted in the 2020 NRA, the *"Administration des douanes et accises"* (ADA) is Luxembourg's customs administration. Since the entry into force of the 2021 Cash Control Law, the ADA has the power to detain undeclared or undisclosed cash equal to or greater than EUR 10 000, or cash suspected as crime proceeds or instrumentalities, transported across the borders of Luxembourg for 30 days. Upon assessing proportionality and necessity, the 30 days may be prolonged to 90 days. With the 2021 Cash Control Law and Regulation (EU) 2018/1672[383], cross-border cash transport equal to or greater than EUR 10 000 covers highly liquid stores of value as defined in Annex I of Regulation (EU) 2018/1672. Furthermore, extra-EU and intra-EU cross-border cash transports are handled identically, meaning a cash declaration is mandatory in both cases. For unaccompanied cash (e.g. sent via courier express or postal consignments), the sender, the recipient or the representative thereof must submit a disclosure declaration within 30 days, at the latest upon invitation by the customs officer when the cash has been detected. When establishing an infringement against the cash control legal framework, the ADA's officers draw up a penal report and emit an administrative decision to detain the cash for 30 days. This decision is subject to an appeal at the Administrative Tribunal. The penal report is submitted to the Prosecutor's Office and to the CRF. The Prosecutor's Office may request a seizing order by the investigative judge, which once granted, overrides the administrative decision to detain.

The number of cross-border cash declarations (relating to currency and bearer negotiable instruments) submitted to the ADA were quite stable over the past three years.

### *7.4.3. Administration des contributions directes*

The *"Administration des contributions directes"* (ACD), Luxembourg's direct tax administration plays an important role in supporting detection efforts. The ACD has relevant tax review processes in place and information sharing with national and international authorities that contributes to reducing the likelihood of tax crimes and increase the probability of detection should these occur. Requests from its foreign counterpart relate to BO information, bank information, accounting records, and legal ownership. Moreover, the ACD established an international cooperation department to facilitate international cooperation.

[383] Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005.

## 7.5. Prosecution, investigation, asset recovery and asset management

During the observation period, the majority of investigations, prosecutions and convictions concerned fraud and forgery, drug trafficking, and robbery and theft.

Explanations relating to the role and mandate of prosecution authorities, and investigative judges explained in 2020 NRA continue to be relevant for the observation period of this NRA.

**Insight Box 24: Extract of the 2020 NRA (Section 7.1 "Overview of mitigating factors")**

**Prosecution authorities** conduct all necessary actions to investigate and prosecute criminal offenses and recover crime-related assets. The General State Prosecutor ("Procureur général d'Etat") represents the prosecution authorities in person or through his or her deputies before the Court of Cassation and the Court of Appeal. The State Prosecutors represent in person or through their substitutes the prosecution authorities before the District Courts and the Police Courts. The State Prosecutors receive complaints and denunciations (including dissemination reports from the CRF) and assess the action to be taken on them. They take or cause to be taken all necessary steps to ascertain the truth and to prosecute violations of criminal law. The State Prosecutors supervise to this end the activities of the Judicial Police Service (SPJ) in preliminary investigations and may transfer the case to an investigative judge to conduct a judicial inquiry if coercive measures are required or if the offence is a crime that cannot be decriminalised (based on a "requisition").

**Investigative judges** are not part of the prosecution authorities and, as such, remain independent. investigative judges may order measures that restrict individual freedoms (i.e. coercive measures) such as provisional detention, searches and seizures. The SPJ executes the investigations as per orders of State prosecutors or investigative judges, and can use a wide range of investigative techniques (including undercover operations, intercepting communications, accessing computer systems, etc.), if ordered to do so. Investigative judges have the means to access or request relevant information within inquiries, including to the financial sector. The powers of investigative judges, when providing major mutual legal assistance, and State Prosecutors, when providing ancillary mutual legal assistance, are identical for both domestic and foreign cases. In fact, given Luxembourg's open economy and significant share of international funds, a considerable part of their activities relates to mutual legal assistance (MLA) and other forms of international cooperation (such as among asset recovery offices).

Moreover, it is worth noting that the SPJ has a dedicated AML unit specialized in ML, TF, circumvention of financial restrictions and the identification and tracing of criminal assets, that is distinct from the units in charge of either organised crime or drug trafficking cases. Upon request or in major/complex cases, a parallel financial investigation regarding the ML and asset recovery component is done by the AML unit, in close collaboration with the other unit that investigates the predicate offence.

It should be highlighted that due to the increasing complexity of ML/TF cases, it is crucial to continue to equip these authorities with the necessary resources to effectively tackle these cases.

**Insight Box 25: Law of 24 July 2024**

The Law of 24 July 2024 created 94 vacancies and set up a three-year recruitment plan for magistrates in Luxembourg. Among those 94 vacancies:

- 32 additional vacancies were created for judges within the Luxembourg District Court;
- 22 additional vacancies were created for judges within the State Prosecutor's Office of the Luxembourg District Court;
- 11 additional vacancies were created for judges within the Diekirch District Court;
- 5 additional vacancies were created for judges within the State Prosecutor's Office of the Diekirch District Court;
- 6 additional vacancies were created for magistrates for the CRF.

The same law foresees the creation of 20 vacancies for *"attachés de justice"*.

As for the SPJ, the 2023-2028 Coalition Agreement[384] emphasizes the need to strengthen its ressources as to ensure (i) the effective enforcement of AML laws and of supranational recommendations following the FATF mutual evaluation exercise in 2023. The government thus grants to the department in charge of the fight against economic and financial crimes of the SPJ an extraordinary recruitement plan amounting to 40 civilian investigators from the A1/A2 career until the year 2026, in addition to the ordinary recruitment of civilian or police investigators and staff[385].

During the observation period, the Asset Management Office (*"Bureau de Gestion des Avoirs"*, AMO) was established and the powers of the Asset Recovery Office ("*Bureau de Recouvrement des Avoirs",* ARO) have been strengthened, in line with Luxembourg's "crime does not pay" policy, which aims to combat economic crime by depriving criminals of the benefits of their offenses. These changes are outlined in the sub-sections below.

### *7.5.1. Asset Management Office*

The Law of 22 June 2022 on the management and recovery of seized or confiscated assets established the Asset Management Office (AMO), whose mission includes the mandatory management of all sums, whether cash or credited account balances, credit or VAs seized in the course of domestic or foreign criminal proceedings. The judicial authorities may also entrust the AMO with the management of all other property, whatever its nature, whose conservation in kind is not necessary for the determination of the truth and which requires management acts for its conservation or valuing, seized in the course of national or foreign criminal proceedings. At the request of the State Prosecutor, it also manages confiscated assets. Furthermore, the AMO also ensures, on the instructions of the judicial authorities, the disposal or destruction of seized property. It is also in charge of the centralization and computerized management of data relating to all seized and confiscated goods, and which do not constitute evidence.

[384] Luxembourg Government, *Accord de coalition 2023-2028,* link.

[385] To be eligible for an A1 or A2 career, a university degree is required.

The AMO organizes training and information activities striving to raise awareness on its tasks and to promote good practices with regard to seizures and confiscation in criminal matters.

Lastly, the AMO negotiates agreements with foreign authorities for the sharing of property confiscated on the basis of a foreign decision.

Since the AMO became operational on 1 October 2022, it has negotiated 13 agreements with foreign authorities. The table below provides statistics relating to seized credit accounts, security accounts and cash[386]:

**Table 31: Seized amounts managed by the AMO. Amounts in million euros**

| Amounts as at: | Credit balances | | Securities accounts | | Sum of credit balances (cash) and securities accounts | | |
|---|---|---|---|---|---|---|---|
| | Foreign cases | Domestic cases | Foreign cases | Domestic cases | Total | Total foreign *(% total)* | Total domestic *(% total)* |
| 01/10/2022[387] | 299,095 | 75,981 | 288,340 | 143,825 | 807,241 | 587,435 *(73%)* | 219,806 *(27%)* |
| 31/12/2022 | 7,746 | 1,476 | 1,808 | 0 | 11,030 | 9,544 *(87%)* | 1,476 *(13%)* |
| 31/12/2023 | 55,481 | 69,217 | 17,189 | 5,225 | 147,112 | 72 670 *(49%)* | 74 442 *(51%)* |

### *7.5.2. Asset Recovery Office*

As noted in the 2020 NRA, the Asset Recovery Office (ARO) is part of the State Prosecutor's Office at the Luxembourg District Court and is responsible for identifying and tracing assets linked to foreign crimes, facilitating the exchange of information with foreign authorities and advising prosecution authorities, investigative judges and the SPJ on measures to take within investigations of foreign crimes.

In 2023, the ARO concluded in 2023 a cooperation agreement with the CSSF concerning the ARO's access to the register of IBAN accounts and safe-deposit boxes held by credit institutions in Luxembourg. As a result, the ARO now has direct and effective access to this register.

## 7.6. International cooperation

International cooperation remains at the centre of Luxembourg's AML/CFT approach given its open economy and diverse working population. This is ensured at the level of each competent authority (via membership in relevant international groups, as well as through information sharing mechanisms), law enforcement agencies (police cooperation), prosecution authorities and investigative judges (MLA requests and European Arrest Warrants (EAW), European Investigation Orders (EIO)), the MoJ (extraditions) and exchanges with other Asset Management and Asset Recovery Offices, as well as international conventions and bilateral and multi-lateral treaties.

[386] AMO, *Rapport d'activité 2022-2023*, link.

[387] The AMO started operations on 1 October 2022.

During the observation period, Luxembourg received over 2 700 MLA requests regarding coercive measures and over 3 800 MLA requests regarding non-coercive measures. About 90% of MLA requests requiring coercive measures originated from other EU countries. Luxembourg's most frequent counterparts were Germany, France, and Belgium. Luxembourg also received and executed many additional/subsequent MLA requests aiming at gathering additional evidence. Between 2020 and 2023, Luxembourg received over 900 additional requests.

For MLA requests that concern economic or financial crimes, the execution of coercive measures (e.g. searches, seizures, etc.) upon decision of the prosecution authorities or the investigative judge is generally assisted by a dedicated unit within the SPJ. The aforementioned unit employs 16 experienced investigators by 2023, each of which processes on average 50 incoming MLA requests per year.

As shown in the table below, the CRF actively seeks and receives requests from and to foreign counterparts:

**Table 32: CRF number of incoming and outgoing requests for information, 2020 - 2023**

| | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|
| **Number of outgoing requests for information** | 1 174 | 1 098 | 1 130 | 757 |
| **Number of incoming requests for information** | 567 | 694 | 631 | 643 |
| **Number of executed incoming requests for information** | 567 | 694 | 631 | 643 |

In addition to the number of cases that have been disseminated to the CRF's foreign counterparts (see the table above), the following table summarizes the number of international cross-border disseminations (XBD) and cross-border reporting (XBR) exchanges for the years 2020 to 2023 between the CRF and FIUs of other EU Member States. It should be noted that the number of these cross-border exchanges can be used be used in parallel with traditional international cooperation.

**Table 33: Exchanges XBD and XBR, 2020 - 2023[388]**

| | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|
| **Exchanges "cross border reporting" (XBR)** | 26 557 | 24 216 | 24 339 | 24 371 |
| **Exchanges "cross border dissemination" (XBD)** | 1 222 | 1 460 | 3 377 | 2 412 |

In a similar vein, the CRF implemented 633 freezing measures for a total amount of over EUR 1 billion.

**Table 34: CRF freezing measures, 2020 - 2023[389]**

| | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|
| Number of freezing orders | 291 | 96 | 93 | 153 |
| Amounts frozen (in EUR) | 223 924 013,14 | 38 221 309,28 | 180 220 553 | 609 407 048 |

[388] *La Justice en chiffres*, 2021, link, 2022, link and 2023, link.

[389] CRF, *Rapport annuel,* 2021-2022, link and CRF, *Rapport annuel*, 2023, link.

# 8. Residual risk

The residual risk level is used to identify areas where Luxembourg remains exposed to ML 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 framework and further reduce the ML risk. The table below provides an overview of the inherent residual risk by sub-sector assessed in this NRA update.

**Table 35: Residual ML risk assessment at the sub-sector level**

| Sector | Sub-sector | 2025 NRA: Inherent risk | 2025 NRA: Residual risk |
|---|---|---|---|
| Banks | Retail and business banks | High | Medium |
| | Entities operating online | High | Medium |
| | Wholesale, corporate and investment banks | High | Medium |
| | Private banking | Very High | Medium |
| | 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[390] | High | 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[391] | High | 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[392] | Medium | Low |
| | Collective investments | Medium | Medium |
| | CSSF-supervised pension funds | 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 providing corporate services | High | Medium |

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

| Sector | Sub-sector | 2025 NRA: Inherent risk | 2025 NRA: Residual risk |
|---|---|---|---|
| Specialised PFSs | Professional depositaries | Medium | Low |
| Support PFSs and other specialised PFSs[393] | Support PFSs | Very Low | Very Low |
| | Other specialised PFSs | | |
| Market operators | | Low | Low |
| Insurance | Life insurance | High | Medium |
| | Non-life insurance | Low | Low |
| | Reinsurance | Low | Low |
| | Intermediaries | Medium | Low |
| | Professionals of the insurance sector (PSAs) | Low | Very Low |
| | CAA-supervised pension funds | Very Low | Very Low |
| Real estate agents and developers | Real estate agents *(agents immobiliers)* | High | Medium |
| | Real estate developers *(promoteurs immobiliers)* | High | Medium |
| Freeport operators | | Medium | Low |
| Dealers in goods | Precious metals/jewellers/clocks | Medium | Low |
| | Car dealers | High | Medium |
| | Art/Antiques | Medium | Low |
| | Luxury goods (e.g. *"maroquinerie")* | Medium | Medium |
| Gambling service providers | Casino | Medium | Very Low |
| | National lottery | Low | Very Low |
| Legal and accounting professions supervised by the AED | Accountants | High | High |
| | Professional directors and business centres | High | High |
| Legal and accounting professions | Lawyers | High | Medium |
| | Notaries | High | Medium |
| | Court bailiffs *(huissiers de justice)* | Medium | Medium |

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

| Sector | Sub-sector | 2025 NRA: Inherent risk | 2025 NRA: Residual risk |
|---|---|---|---|
| supervised by SRBs | Audit profession[394] | Medium | Low |
| | Chartered professional accountants *(experts-comptables)* | High | Medium |
| Legal persons and legal arrangements | *Sociétés commerciales* | Very High | Medium |
| | *Sociétés civiles* | Medium | Low |
| | NPOs (as per FATF definition) carrying out primarily international activities – ASBLs and *Fondations*[395] | High | High |
| | NPOs (as per FATF definition) carrying out local activities – ASBLs[396] | Low | Low |
| | NPOs (as per FATF definition) carrying out local activities – *Fondations*[397] | Low | Very Low |
| | Other legal persons | High | Medium |
| | Domestic *Fiducies* | Very High | Very High |
| | Foreign trusts | Very High | Very High |

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

[395] This category corresponds to "*Associations sans but lucrative* (ASBL) and *fondations* with Non-governmental organisations (NGO) status" in NRA 2020.

[396] This category corresponds to "Other *associations sans but lucratif* (ASBL)" in NRA 2020. Note than in NRA 2020, it included ASBLs in and out of the FATF NPO definition (i.e. 8 000 vs. 100 ASBLs falling in FATF NPO definition). In this respect, NRA 2020 noted that "most ASBLs are estimated to have a low exposure to ML/TF threats; but given their relatively high number, the inherent risk is evaluated as medium for the local ASBL sector as a whole until a national assessment of their activities will permit a more granular assessment, in line with a conservative approach".

[397] This category corresponds to "Other *fondations*" in NRA 2020. Note that in NRA 2020, it included *Fondations* in and out of the FATF NPO definition.

## Appendix A. List of predicate offences to ML[398]

| Predicate offence (as per threat assessment) | Law(s) defining the predicate offence, in French | Relevant article(s) within the law (and actual designation in Luxembourg law, in French) | ML predicate offence |
|---|---|---|---|
| Insider trading and market manipulation | Loi modifiée du 23 décembre 2016 relative aux abus de marché (L-23.12.2016) | 18 Abus de marché, délit d'initié | 506-1, tiret 24 CP |
| Smuggling | Loi générale sur les douanes et accises (LGDA) modifiée du 18 juillet 1977 (L-18.07.1977) | 220 et 231 Contrebande | 506-1, tiret 23 CP |
| Counterfeiting and piracy of products | Loi modifiée du 18 avril 2001 sur le droit d'auteur (L-18.01.2001) | 82 à 85 Droits d'auteur | 506-1, tiret 17 CP |
| | Code pénal (CP) | 309 Violation du secret d'affaires | 506-1, tiret 8 CP |
| Corruption and bribery | Code pénal (CP) | 240 Détournement de deniers publics | 506-1, tiret 28 CP |
| | Code pénal (CP) | 243 Concussion à l'aide de violences et menaces | 506-1, tiret 28 CP |
| | Code pénal (CP) | 246 à 253 Corruption active et passive | 506-1, tiret 6 CP |
| Kidnapping, illegal restraint and hostage taking | Code pénal (CP) | 363, 364 et 365 Crimes et délits relatifs aux mineurs | 506-1, tiret 28 CP |
| | Code pénal (CP) | 368 à 370 | 506-1, tiret 3 CP |

[398] CRF, *Rapport annuel,* 2023, link.

| Predicate offence (as per threat assessment) | Law(s) defining the predicate offence, in French | Relevant article(s) within the law (and actual designation in Luxembourg law, in French) | ML predicate offence |
|---|---|---|---|
| | | Enlèvement de mineurs | |
| | Code pénal (CP) | 436, 437 et 438<br>Détention illégale et arbitraire de plus d'un mois : sur faux ordre de l'autorité publique, faux costume ; menace de mort | 506-1, tiret 28 CP |
| | Code pénal (CP) | 442-1, 442-1bis et 442-1 ter<br>Prise d'otages | 506-1, tiret 28 CP |
| Sexual exploitation (including sexual exploitation of children) | Code pénal (CP) | 372 alinea 3, 372bis, 372ter<br>Attentat à la pudeur : avec violence ou menaces ; sur enfant de moins de 16 ans | 506-1, tiret 28 CP |
| | Code pénal (CP) | 379<br>Exploitation de la prostitution | 506-1, tiret 3 CP |
| | Code pénal (CP) | 379bis, 380, 381 et 382-7<br>Proxénétisme | 506-1, tiret 3 CP |
| | Code pénal (CP) | 383, 383bis, 383ter, 384 et 385-2<br>Outrages publics aux bonnes mœurs et dispositions particulières pour protéger la jeunesse | 506-1, tiret 4 CP |
| Extortion | Code pénal (CP) | 470<br>Extorsion | 506-1, tiret 28 CP |
| Fraud and forgery | Code pénal (CP) | 194 à 197<br>Faux en écritures | 506-1, tiret 28 CP |

| Predicate offence (as per threat assessment) | Law(s) defining the predicate offence, in French | Relevant article(s) within the law (and actual designation in Luxembourg law, in French) | ML predicate offence |
|---|---|---|---|
| | Code pénal (CP) | 208<br>Faux certificat commis par un fonctionnaire dans l'exercice de sa fonction ; usage de faux certificat | 506-1, tiret 28 CP |
| | Code pénal (CP) | 210-1<br>Pratiques illicites eu égard aux documents de voyage ou d'identité | 506-1, tiret 28 CP |
| | Code pénal (CP) | 211 et 212<br>Faux commis dans les dépêches télégraphiques | 506-1, tiret 28 CP |
| | Code pénal (CP) | 215 et 216 ; 221 ; 223<br>Faux témoignage et faux serment | 506-1, tiret 28 CP |
| | Loi modifiée du 10 août 1915 concernant les sociétés commerciales (L-10.08.1915) | 1500-8<br>Faux bilans | 506-1, tiret 28 CP |
| | Loi modifiée du 10 août 1915 concernant les sociétés commerciales (L-10.08.1915) | 1500-9<br>Usage de faux bilans | 506-1, tiret 28 CP |
| | Code pénal (CP) | 241<br>Destruction d'actes et de titres | 506-1, tiret 28 CP |
| | Code pénal (CP) | 489 et 490<br>Banqueroute frauduleuse | 506-1, tiret 10 CP |
| | Code pénal (CP) | 491 et 492<br>Abus de confiance | 505-1, tiret 10 CP |
| | Code pénal (CP) | 493 | 506-1, tiret 10 CP |

| Predicate offence (as per threat assessment) | Law(s) defining the predicate offence, in French | Relevant article(s) within the law (and actual designation in Luxembourg law, in French) | ML predicate offence |
|---|---|---|---|
| | | Abus de faiblesse | |
| | Code pénal (CP) | 494<br>Usure | 506-1, tiret 10 CP |
| | Code pénal (CP) | 495<br>Production frauduleuse d'une pièce en justice | 506-1, tiret 10 CP |
| | Code pénal (CP) | 496<br>Escroquerie et tentative d'escroquerie | 506-1, tiret 10 CP |
| | Code pénal (CP) | 496-1 à 496-6<br>Escroquerie à la subvention | 506-1, tiret 5 CP |
| | Loi modifiée du 10 août 1915 concernant les sociétés commerciales (L-10.08.1915) | 1500-11<br>Abus de biens sociaux | 506-1, tiret 28 CP |
| | Code pénal (CP) | 506<br>Recel de biens obtenus à l'aide d'un crime ou délit | 506-1, tiret 28 CP |
| | Code pénal (CP) | 507<br>Destruction ou détournement frauduleux d'objets immobiliers | 506-1, tiret 28 CP |
| Counterfeiting currency | Code pénal (CP) | 161 ; 166 ; 167 ; 169 ; 170 ; 173 et 176<br>Fausse monnaie | 506-1, tiret 28 CP<br>506-1, tiret 8 CP |
| Tax crimes | Loi générale des impôts modifiée (LGI) du 22 mai 1931 (L-22.05.1931) | § 396 alinéas (5) et (6)<br>Fraude fiscale aggravée et escroquerie fiscale en matière d'impôts directs | 506-1, tiret 25 CP |

| Predicate offence (as per threat assessment) | Law(s) defining the predicate offence, in French | Relevant article(s) within the law (and actual designation in Luxembourg law, in French) | ML predicate offence |
|---|---|---|---|
| | Loi modifiée du 28 janvier 1948 tendant à assurer la juste et exacte perception des droits d'enregistrement (L-28.01.1948) | 29, alinéa 1 et 2<br>Fraude fiscale aggravée et escroquerie fiscale en matière de droit d'enregistrement | 506-1, tiret 26 CP |
| | Loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée<br>(L-12.02.1979) | 80, paragraphe 1er<br>Fraude fiscale aggravée et escroquerie fiscale en matière de TVA | 506-1, tiret 27 CP |
| Environmental crime | Loi modifiée du 18 juillet 2018 concernant protection de la nature et des ressources naturelles<br>(L-18.07.2018) | 75 | 506-1, tiret 18 CP |
| | Loi modifiée du 21 juin 1976 relative à la lutte contre la pollution de l'atmosphère<br>(L-21.06.1976) | 9 | 506-1, tiret 19 CP |
| | Loi modifiée du 10 juin 1999 relative aux établissements classés<br>(L-10.06.1999) | 25 | 506-1, tiret 20 CP |
| | Loi modifiée du 19 décembre 2008 relative à l'eau<br>(L-18.12.2008) | 61 | 506-1, tiret 21 CP |
| | Loi modifiée du 21 mars 2012 relative à la gestion des déchets<br>(L-21.03.2012) | 47 | 506-1, tiret 22 CP |
| Murder, grievous bodily injury | Code pénal (CP) | 101 à 112<br>Des attentats et des complots contre le (Roi) Grand-Duc, contre la famille royale grand- | 506-1, tiret 28 CP |

| Predicate offence (as per threat assessment) | Law(s) defining the predicate offence, in French | Relevant article(s) within the law (and actual designation in Luxembourg law, in French) | ML predicate offence |
|---|---|---|---|
| | | ducale et contre la forme du Gouvernement | |
| | Code pénal (CP) | 112-1<br>Attentat contre les personnes jouissant d'une protection internationale | 506-1, tiret 1 CP |
| | Code pénal (CP) | 136bis à 136 quinquies<br>Violations graves du droit humanitaire international | 506-1, tiret 28 CP |
| | Code pénal (CP) | 260-1 à 260-4<br>Torture | 506-1, tiret 28 CP |
| | Code pénal (CP) | 348 et 352<br>Avortement | 506-1, tiret 28 CP |
| | Code pénal (CP) | 356-357 ; 360<br>Exposition et délaissement d'enfant | 506-1, tiret 28 CP |
| | Code pénal (CP) | 375 et 376<br>Viol | 506-1, tiret 28 CP |
| | Code pénal (CP) | 393 à 397<br>Meurtre, assassinat, parricide, infanticide, empoisonnement | 506-1, tiret 28 CP |
| | Code pénal (CP) | 400 et 401<br>Coups et blessures volontaires : maladie incurable ; incapacité permanente ; perte organe ; mutilation ; mort | 506-1, tiret 28 CP |

| Predicate offence (as per threat assessment) | Law(s) defining the predicate offence, in French | Relevant article(s) within the law (and actual designation in Luxembourg law, in French) | ML predicate offence |
|---|---|---|---|
| | Code pénal (CP) | 401bis<br>Coups et blessures volontaires sur enfant moins 14 ans accomplis | 506-1, tiret 28 CP |
| | Code pénal (CP) | 403 et 404<br>Empoisonnement : maladie incurable ; incapacité permanente ; perte organe ; mort | 506-1, tiret 28 CP |
| | Code pénal (CP) | 406, 407 et 408<br>Entrave à convoi ferroviaire : maladie ; incapacité de travail ; maladie incurable ; incapacité permanente ; perte organe ; mutilation grave | 506-1, tiret 28 CP |
| | Code pénal (CP) | 409 paragraphes 2 à 5 et 409 bis paragraphes 1,3 et 4<br>Coups et blessures sur conjoint : préméditation ; maladie ; incapacité temporaire ; maladie incurable ; incapacité permanente ; perte organe ; mutilation grave ; mort | 506-1, tiret 28 CP |
| | Code pénal (CP) | 430<br>Duel | 506-1, tiret 28 CP |
| | Code pénal (CP) | 438 | 506-1, tiret 28 CP |

| Predicate offence (as per threat assessment) | Law(s) defining the predicate offence, in French | Relevant article(s) within the law (and actual designation in Luxembourg law, in French) | ML predicate offence |
|---|---|---|---|
| | | Séquestration illégale-torture-maladie incurable-mort | |
| | Code pénal (CP) | 474 et 475<br>Vol commis à l'aide de violences et menaces : mort ; meurtre commis pour faciliter le vol ou l'extorsion ou pour en assurer l'impunité | 506-1, tiret 28 CP |
| | Code pénal (CP) | 510 à 513, 518, 521, 525, de 529 à 532 et 547<br>Destruction volontaire d'objets mobiliers d'autrui : violences ou menaces ; maladie ; lésion corporelle ; meurtre | 506-1, tiret 28 CP |
| | Loi modifiée du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine (L-25.11.1982) | 18 | 506-1, tiret 16CP |
| Participation in an organised criminal group and racketeering | Code pénal (CP) | 322 à 324quater<br>Association de malfaiteurs et organisation criminelle | 506-1, tiret 2 CP |
| Piracy | Loi modifiée du 14 avril 1992 instituant un code disciplinaire et pénal pour la marine (L-14.04.1992) | 65-1 | 506-1, tiret 28 CP |
| Illicit arms trafficking | Loi modifiée du 15 mars 1983 sur les armes et munitions (L-14.03.1983) | 28 | 506-1, tiret 7 CP |

| Predicate offence (as per threat assessment) | Law(s) defining the predicate offence, in French | Relevant article(s) within the law (and actual designation in Luxembourg law, in French) | ML predicate offence |
|---|---|---|---|
| Illicit trafficking in stolen and other goods | Loi du 25 février 2022 relative au patrimoine culturel (L-25.02.2022) | 118 et 119 | 506-1, tiret 14 CP |
| Drug trafficking | Loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie (L-19.02.1973) | 8.1 a) et b) | 8-1 L-19.02.1973 |
| | Loi du 11 janvier 1989 réglant la commercialisation des substances chimique à activité thérapeutique (L-11.01.1989) | 5 | 506-1, tiret 15 CP |
| Trafficking in human beings and migrant smuggling. | Code pénal (CP) | 382-1 et 382-2<br>Traite des êtres humains | 506-1, tiret 3 CP |
| | Code pénal (CP) | 382-4 et 382-5<br>Trafic illicite des migrants | 506-1, tiret 3 CP |
| Robberies or theft | Code pénal (CP) | 463 ; 464<br>Vol simple, vol domestique | 506-1, tiret 9 CP |
| | Code pénal (CP) | 467 à 469 ; 471 à 476<br>Vol qualifié | 506-1, tiret 28 CP |
| Cybercrime | Code pénal (CP) | 509-1 à 509-7<br>Certaines infractions en matière informatique | 506-1, tiret 11 CP |
| | Loi du 14 août 2000 relative au commerce électronique (L-14.08.2000) | 48<br>Spam | 506-1, tiret 12 CP |
| | Loi modifiée du 30 mai 2005 relative au traitement illicite des données à caractère personnel dans le secteur des communications électroniques (L-30.05.2005) | 11 | 506-1, tiret 13 CP |

# Appendix B. Methodology

## B.1. Vulnerabilities methodology

**Table 36: Scorecard of assessment criteria for sectorial vulnerabilities**

| Dimension | Sub-dimension | Examples of indicators/data |
|---|---|---|
| **Structure** | Size | • Revenue/turnover and profit<br>• Assets<br>• Assets under management |
| | Fragmentation/complexity | • Number of institutions<br>• 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 risky countries based on FATF lists)<br>• % of entities with foreign mother |
| **Products/ activities** | Products/activities | • % of high-risk products (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 FATF list of geographies with weak AML/CFT measures (e.g. in clients revenue, assets, transactions) |
| **Clients/ transactions** | Volume | • Number of clients<br>• Total number (stock)<br>• New clients per year (flow) |
| | Risk | • % high-risk clients (based on supervised entities' internal models)<br>• % PEPs (over time): domestic vs. foreign |
| **Channels** | Channels | • Type of interaction: % face-to-face, indirect (e.g. online), via intermediaries |

**Table 37: 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 38: Inherent risk scorecard risk – overall inherent risk outcome**

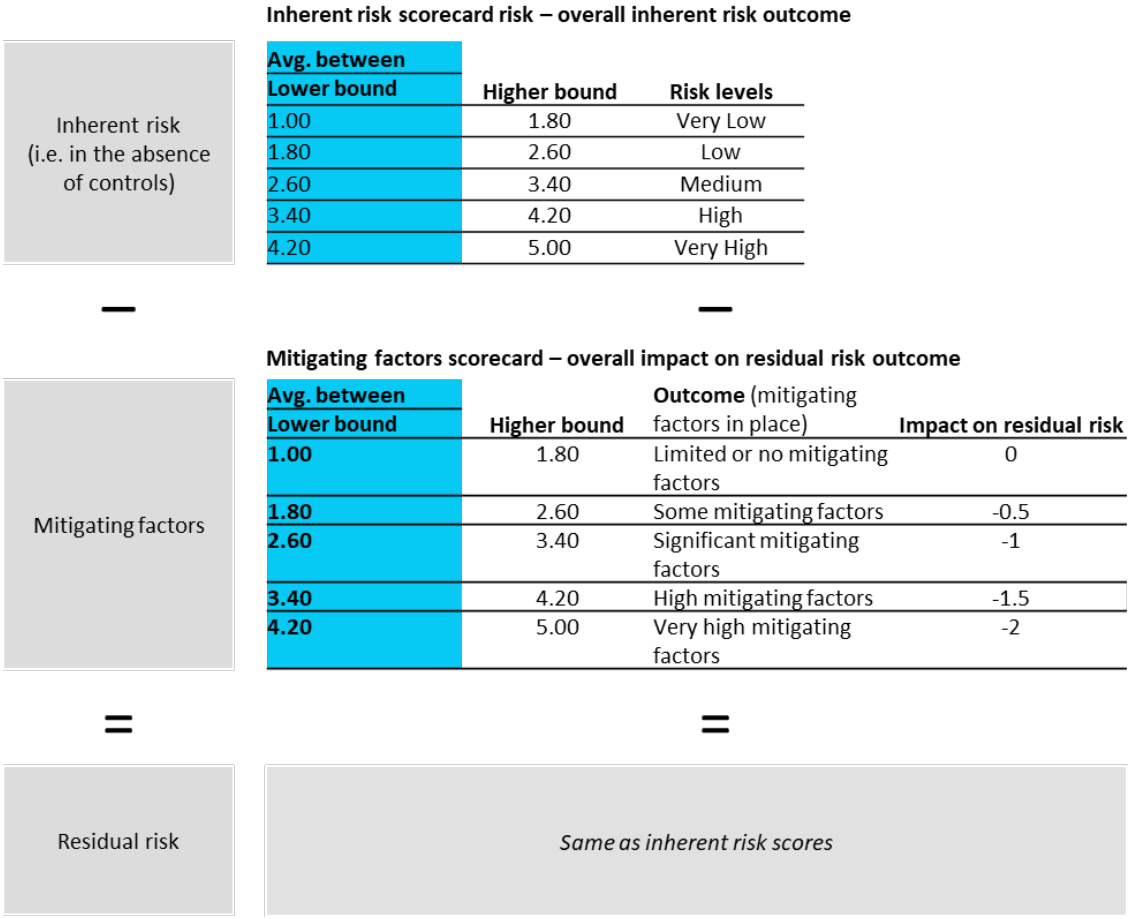
| Average between | | |
|---|---|---|
| **Lower bound** | **Higher bound** | **Risk levels** |
| 1,00 | 1,80 | Very Low |
| 1,80 | 2,60 | Low |
| 2,60 | 3,40 | Medium |
| 3,40 | 4,20 | High |
| 4,20 | 5,00 | Very High |

## B.2. Mitigating factors and residual risk methodology

**Table 39: 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 ML risks and AML/CFT obligations | • Annual questionnaires<br>• Risk assessments (e.g. entity level, sub-sector risk assessments)<br>• Internal trainings<br>• Supervisors' publications on ML/TF risks in the sector |
| | Regulation & information | • Type of supervisor (e.g. association, ministry, dedicated supervisor)<br>• Regulation communication to the sector (e.g. circulars)<br>• Education to private sector (e.g. publications, trainings, etc.) |
| **Prevention / Private sector controls** | ML controls in place | • CDD/KYC approach, aligned with risk level, number of customers declined based on CDD<br>• 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<br>• 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)<br>• Supervisor procedures formalised and up to date |
| | Enforcement | • Remedial actions imposed (i.e. number of sanctions and other actions)<br>• 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<br>• Quality of STRs and SARs issued by subsector and predicate offences |

**Figure 32: Residual risk calculation**




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".

These residual risks outcomes are presented in the residual risk assessment section further below.

# Appendix C. List of tables, figures, case studies and insight boxes

## C.1. List of tables

## C.2. List of figures

## C.3. List of case studies



## C.4. List of insight boxes

# Appendix D. 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 et de la TVA |
| AEOI | Automatic exchange of information |
| 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 |
| CEF | Cyber-enabled fraud |
| CPA | Chartered professional accountants |
| CRF | Cellule de renseignement financier |
| CRS | Common Reporting Standard |
| CSAE | Child sexual abuse and exploitation |
| CSAM | Child sexual abuse material |
| CSD | Central Securities Depositories |
| CSSF | Commission de Surveillance du Secteur Financier |
| DDoS | Distributed denial of service |
| DESI | Digital Economy and Society Index |
| DNFBP | Designated non-financial businesses and professions |
| EAW | European Arrest Warrant |
| EBA | European Banking Authority |
| ECB | European Central Bank |
| ECSP | European Crowdfunding Service Provider |
| EFTA | European Free Trade Association |
| EIO | European Investigation Order |
| EMI | E-money institution |
| EMPACT | European Multidisciplinary Platforms Against Criminal Threats |
| EOIR | Exchange of information on request |
| EPPO | European Public Prosecution Office |
| EU | European Union |
| FATF | Financial Action Task Force |
| FCP | Fonds commun de placement |

| Acronym | Definition |
|---|---|
| FDI | Foreign direct investment |
| FI | Financial institution |
| FIU | Financial intelligence unit |
| FMCG | Fast moving consumer goods |
| GDP | Gross domestic product |
| GGR | Gross gaming revenue |
| HOSSP | Hawala and other similar service providers |
| IMF | International Monetary Fund |
| IRE | Institut des Réviseurs d'Entreprises |
| ISC | Inter-ministerial Steering Committee for the Fight against Money Laundering and Terrorist Financing |
| KYC | Know your customer |
| LBR | Luxembourg Business Registers |
| LEA | Law enforcement authorities |
| 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 |
| MFF | Multiannual Financial Framework |
| 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 |
| MoU | Memorandum of Understanding |
| MTIC | Missing Trader Intra Community |
| MVTS | Money value or 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 |
| 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 |

| Acronym | Definition |
|---|---|
| RRF | Recovery and Resilience Facility |
| SA | Société anonyme |
| SARL | Société à responsabilité limitée |
| SCSpé | Sociétés en commandite spéciale |
| SICAV | Société d'investissement à capital variable |
| SME | Small and medium-sized enterprises |
| 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 |
| SOCTA | Serious Organised Crime Threat Assessment |
| SPACE | Study on the payment attitudes of consumers in the euro area |
| SRB | Self-regulatory body |
| STOR | Suspicious order and transaction report |
| STR | Suspicious transaction report |
| TCSP | Trust and corporate service provider |
| TF | Terrorist financing |
| UCITS | Undertaking for collective investment in transferable securities |
| UHNW | Ultra-High-Net-Worth Individual |
| VA | Virtual asset |
| VASP | Virtual asset service provider |
| VAT | Value added tax |
| vIBAN | Virtual IBAN |