THE GOVERNMENT
OF THE GRAND-DUCHY OF LUXEMBOURG
Ministry of Finance

PF AND TF TFS VRA

Luxembourg's Vertical Risk Assessment into Proliferation Financing and Terrorist Financing Targeted Financial Sanctions

Observation period: 2018-2023

June 2026

Contents

1. Executive Summary

1.1. Introduction, context and methodology

Weapons of Mass Destruction ("WMD") pose a serious threat to international peace, security, and human life, and preventing the financing of proliferation is central to reducing this threat. Targeted Financial Sanctions ("TFS") are a key mechanism used by the United Nations ("UN"), as well as other supranational and national authorities, to mitigate this risk. According to the Financial Action Task Force ("FATF"), the financing of proliferation refers to "*the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes).*"[1]

The scope of Proliferation Financing (PF) is broad and detecting PF activity can be highly challenging. The PF "value chain" consists of three parts: (1) raising funds (whether legally or illegally) for the proliferation activity; (2) obscuring or moving funds by disguising and transferring them into the international financial system; and (3) using funds to acquire goods, materials, technology and the logistics required to fund a country's WMD programme[2]. Organisations may be involved directly or indirectly in the different elements of this chain.

Counter-proliferation financing was first introduced into the mandate of the FATF in 2012[3]. However, the importance of countering PF was reiterated in 2020, when FATF Recommendation 1 (focused on a risk-based approach) and FATF Recommendation 2 were extended to cover PF. The updated Recommendation 1 also provided greater clarity on the definition of PF risk, which is recorded *"strictly and only"* as "*the potential breach, non-implementation or evasion of the targeted financial sanctions obligations"* (obligations mentioned in FATF Recommendation 7)[4].

In addition to PF, this risk assessment also considers TFS related to terrorism financing ("TF"). This is because financial sanctions are also used to address the risks associated with TF, as outlined by FATF Recommendation 6. Given that TF risks were analysed in Luxembourg's Terrorist Financing Vertical Risk Assessment ("TF VRA")[5] and are in the process of being further analysed as part of the ongoing Terrorist Financing national risk assessment, this document focuses only on threats and vulnerabilities related to TF TFS.[6]

TFS are restrictive measures which seek to "*maintain or restore international peace and security*"[7] by restricting dealings with certain States, entities and individuals. They are defined by FATF as "*both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities"*[8] and can vary in scope, sanctioning authority and sanctioned actor.

---

[1] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021 (link)

[2] J. Brewer, *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation, CNAS*, 2018 (link)

[3] RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment*, 2019 (link)

[4] FATF, *Recommendations,* Recommendation 1, 2020 (link)

[5] Luxembourg, *Terrorist Financing Vertical Risk Assessment* ("*Assessing terrorist financing vulnerable sectors*"), 2022 (link)

[6] To note, operators' obligations regarding TF are broader than for PF (e.g. including submission of STRs, where suspicions arise); these dimensions are not considered here but are referenced in the TF VRA.

[7] United Nations Security Council, *Sanctions*, accessed July 2025 (link)

[8] FATF, *International Best Practices Targeted Financial Sanctions related to terrorism and terrorist financing (Recommendation 6)* (page 3), 2013 (link)

This vertical risk assessment ("VRA"), which as mentioned focuses on TFS, looks at the risks associated with potential breach, non-implementation or evasion of TFS against PF and TF in Luxembourg. The basis of this is FATF Recommendations 1 and 2, as well as FATF Recommendations 6 and 7 and associated Immediate Outcomes 10 and 11. The assessment takes "sanctions" (also referred to as "restrictive measures") to mean all TFS that relate to PF and TF and are applicable in Luxembourg (including UN,[9] EU and Luxembourg[10] sanctions). This captures sanctions against the Islamic Republic of Iran ("Iran") and the Democratic People's Republic of Korea ("DPRK"; also called "North Korea") for PF, as well as Al-Qaida (also called "Al-Qaeda"), the Taliban and the Islamic State of Iraq and the Levant ("ISIL"; also called "Daesh" and "Da'esh") for TF. Although not listed in FATF's Recommendation 6, this report also extends the scope of countries for TF to include several EU sanctions regimes: Central African Republic, Iran, Iraq, Libya, Mali, Myanmar, Somalia, South Sudan, Sudan, Syria, Yemen, and the Democratic Republic of Congo. Alongside DPRK, these countries are collectively referred to as "in-scope" countries.

1.2. Assessment of inherent risk and mitigating factors

Luxembourg's exposure to the potential breach, non-implementation or evasion of TFS arises primarily from the importance of its cross-border financial flows and international business activities. Whilst direct links to in-scope countries are very limited, the increasingly circuitous nature of sanctions evasion puts Luxembourgish entities at risk of being inadvertently involved in complex PF/TF pathways. To a lesser extent, it is also exposed via its NPOs and trade flows, which could include goods used for proliferation activity. However, the exact threat varies by type and nature of activity (whether PF or TF).

For PF, Luxembourg's large financial sector and the importance of its legal entities in international business may expose it to threats from DPRK and/or Iran. DPRK is prominent in its active and intentional development of proliferation capacity, and as such is subject to a comprehensive suite of sanctions by the UN. Their methods are often highly creative and sophisticated and rely on elaborate schemes[11]. In particular, DPRK is known for its extensive use of large networks of front and shell companies[12], but other typologies include cyberattacks as a fund-raising mechanism[13] and engaging in sanctions evasion techniques at sea including ship-to-ship transfers[14]. Such techniques have also been observed in Iran-related cases, although the linked geographies may differ[15].

For TF, there is greater diversity in the type of actors that pose a threat to Luxembourg and thus the techniques and typologies used to breach or evade sanctions vary. In line with the TF VRA, actors include international terrorist organisations, as named in UN sanctions lists (Al-Qaida, ISIL and the Taliban), as well as foreign terrorist fighters, lone actors and small terrorist cells, state sponsors of terrorism and corporate terrorist groups[16]. That said, globally, typologies include wealthy donors making covert financial transactions, the exploitation of Money or Value Transfer Services ("MVTS") or even informal networks (such as hawala), and other criminal activities to illicitly raise funds in a way that evades sanctions.

---

[9] Security Council Resolutions 1718 (2006), 2087 (2013), 2094 (2013) and 2270 (2016) for DPRK and Security Council Resolution 2231 (2015) for Iran (as listed in FATF Recommendation 7 and interpretative notes)

[10] As of October 2024, Luxembourg has implemented a legal framework in place to designate natural or legal persons.

[11] US, *National Proliferation Financing Risk Assessment* (page 11), 2018 (link)

[12] UN, *Final report of the Panel of Experts submitted pursuant to resolution 2569* (2021), 2022 (link)

[13] UN, *Final report of the Panel of Experts submitted pursuant to resolution 2515* (2020), 2021 (link)

[14] UN, *Final report of the Panel of Experts established pursuant to resolution 2464* (2019), 2020 (link)

[15] For example, in 2019, the US Treasury took action against an Iranian bank for allegedly using a sophisticated network of front companies and agents in Iran, Turkey and the U.A.E. to exchange rials for foreign currencies, a strategy that is considered to be widely employed by Iran. Source: Wall Street Journal, *U.S. Targets 'Vast Network' Evading Iran Sanctions*, 2019 (link). See also: US Treasury, *Iran sanctions*, accessed July 2025 (link)

[16] Luxembourg, *Terrorist Financing Vertical Risk Assessment* ("*Introduction*"), 2022 (link)

The risk assessment also provides an overview of the vulnerabilities of different sectors in Luxembourg. Most sectors that featured in Luxembourg's national risk assessment ("NRA") of 2020 were assessed at a high inherent risk level, with some then selected for a deep-dive analysis. The deep-dive analysis focused on sectors that are internationally considered as high risk (e.g. as per FATF guidance and/or UN Panel of Expert ("PoE") reports) and that were identified as higher risk in Luxembourg's 2020 NRA[17]. The following table depicts the inherent and residual risk levels for the above-mentioned sectors and subsectors regarding PF and TF TFS. Sub-sectors in grey were not selected for deep-dive analysis.

Table 1: Inherent and residual PF and TF TFS risk assessment at the sector and subsector level

Sector	Inherent risk	Residual risk	Sub-sectors[18]
Banks	**Medium**	**Low**	Retail and business banks (including entities operating online)
	High	**Medium**	Wholesale, corporate and investment banks
	Medium	**Low**	Private banking
	Medium	**Low**	Custodians and sub-custodians (including CSDs)
Investment sector – collective investments	**Medium**	**Low**	Collective investments
Investment sector – wealth managers	**Medium**	**Low**	Wealth managers (*gérants de fortune*)[19]
Investment sector – other			*Brokers dealers*
			Traders/market makers
			Regulated securitisation vehicles
			CSSF supervised pension funds
MVTS	**Medium**	**Low**	Payment institutions (PIs)
	Medium	**Low**	E-money institutions (EMIs)
	Medium	**Low**	Agents and e-money distributors acting on behalf of PIs/EMIs established in another EU Member State
VASPs	**Medium**	**Low**	Virtual asset service providers
Specialised PFSs	**Medium**	**Low**	Specialised PFSs providing corporate services
			Professional depositories
Support PFSs & other specialised PFSs			*Support PFSs*
			Other specialised PFSs
Market operators			*Market operators*
Insurance			*Life insurers*
	Medium	**Low**	Non-life insurers
	Medium	**Low**	Reinsurance
			Intermediaries
			PSA

[17] Luxembourg, *National Risk Assessment*, 2020 (link)

[18] Sub-sectors indicated in italics were not subject to a deep-dive.

[19] The term "wealth managers" herein corresponds to investment firms authorized to carry out the services of investment advice and portfolio management (as per articles 24-4 and 24-5 of the 1993 LSF Law).

Sector	Inherent risk	Residual risk	Sub-sectors[18]
			CAA-supervised pension funds
Legal professions, chartered accountants, statutory auditors, and accountants	**Medium**	**Low**	Lawyers
	High	**Medium**	Notaries
			Bailiffs
	Medium	**Low**	(Approved) statutory auditors and (approved) audit firms (*réviseurs d'entreprises (agréés)* and *cabinets de révision (agréés)*)
	High	**Medium**	Chartered professional accountants (*experts-comptables*)
	High	**Medium**	Accountants
	High	**Medium**	TCSPs – professional directors[20]
	High	**Medium**	TCSPs – business offices
Dealers in high value goods	**Medium**	**Low**	Precious metals, jewelers and clocks
	High	**Medium**	Car dealers
	Medium	**Medium**	Art/antiques
	Medium	**Medium**	Luxury goods
Freeport	**Medium**	**Low**	Freeport operators
Legal persons and legal arrangements	**Very High**	**High**	Sociétés commerciales
	Very High	**Very High**	Domestic "fiducies"
	Very High	**Very High**	Foreign trusts
	Very High	**Very High**	*Associations sans but lucratif* (ASBLs) and *fondations* falling under FATF NPO definition engaged in activities abroad
			Sociétés civiles
			Associations sans but lucratif (ASBLs) and *fondations* falling under FATF NPO definition with local activities
			Other legal entities

The inherent risk assessment for each sector is summarised below. Detailed information on the mitigating factors used by these sectors to reduce inherent risk is provided in the relevant section of the report and not included here given duplication of mitigating factors across different sectors and sub-sectors (e.g. as employed by different competent authorities).

To note that for the banking, investment, MVTS, VASP and Specialised PFS (TCSP) sectors under CSSF supervision, no entity has shareholders from an in-scope country.

Regarding relationships with Iran and DPRK, these sectors were very restrictively exposed in 2023 and thus risks were rather low from a geographical point of view.

Banking: Luxembourg's banking sector is inherently exposed to TFS-related risks due to its international clientele, the products and services it provides, and its distribution model. As of the end of December 2023, the sector consisted of 120 banks with a balance sheet total of €929 billion[21] and a profit before provisions

[20] When the service provided meets the definition of article 1(8)(b) of the 2004 AML/CFT Law.

[21] Luxembourg, *2025 National Risk Assessment of Money Laundering, Observation Period: 2020-2023*, 2025 (link)

and taxes of €8.942 billion[22]. The client base is international[23], albeit links with in-scope countries are more limited[24]. Whilst most banks have a mixed business model, certain products and services have been identified as higher risk, such as wholesale, corporate and investment banking services such as correspondent banking and trade finance[25]. It should be noted that trade finance is not an activity deeply developed by banks in Luxembourg and that correspondent banking activities are concentrated on a few entities. Furthermore, in 2023, two banking entities were registered as Virtual Asset Service Provider (VASP).

Investment sector: Luxembourg's investment sector is exposed to TFS-related risks on account of its size, its global distribution and by the type of investment strategies that are offered. As noted in the sub-sector risk assessment[26], Luxembourg's collective investment sector is the largest in Europe. The aggregated total net assets of Luxembourg funds regulated for AML/CFT purposes diminished from EUR 5,859 billion as of the end of December 2021 to EUR 5,028 billion as of the end of December 2022[27] and increased up to EUR 5,285 billion as of the end of December 2023[28], whereas the overall number of AML/CFT supervised investment funds decreased from 3,492 to 3,377 between 2021 and 2022[29]and increased up to 3,417 between 2022 and 2023. In terms of products, Alternative Investment Funds ("AIFs") present a higher risk because of their target investment classes (notably Private Equity and Real Assets): however, they only account for a small proportion of total net assets. In addition, these products – as well as those services offered by the **wealth management** sub-sector – are largely focused on medium to long-term asset appreciation[30] and therefore are less conducive for actors seeking to breach or evade TFS. More liquid assets such as those related to UCITS (Undertakings for Collective Investment in Transferable Securities) may be more conducive and are open to retail investors, but global typologies related to TFS are less common.

Money Value Transfer Services (MVTS): The inherent risk of the MVTS sector to TFS-related risks is medium in Luxembourg, driven by the sector's size (the volume of transactions processed), product type, clients and distribution model. In 2023, the Grand Duchy was home to 12 e-money[31] and 17 payment institutions[32] that facilitate a large volume of cross-border payments. In 2023, Luxembourg PIs processed 1.5 billion inflows and 0.9 billion outflows (compared to 1.6 billion inflows and 2.3 billion outflows in 2022 and compared to 1.1 billion inflows and 1.1 billion outflows in 2018[33]). The same year, Luxembourg EMIs processed 2.5 billion inflows and 0.17 billion outflows (compared to 2.2 billion inflows and 0.1 billion outflows in 2022 and compared to 1.3 billion inflows and 0.05 billion outflows in 2018[34]). The purely online nature of these services increases inherent risk, as do the multiple different types of services that are provided. Notwithstanding this, financial flows to in-scope countries are very limited.

Virtual Assets Service Providers (VASPs): The inherent risk of the VASPs[35] sector **to TFS-related risks** is medium in Luxembourg, driven mainly by the higher intrinsic exposure of both the services and the virtual assets themselves, the speed of execution of transactions, the distribution channels as VASPs are primarily operating online and the volume processed. In 2023, there were eleven VASPs registered which processed

---

[22] Balance sheet and profit data as of 31 December 2023; data as reported in CSSF's newsletter 279 (link).

[23] Data provided by CSSF.

[24] Data provided by CSSF.

[25] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 27), 2021 (link)

[26] CSSF, *ML/TF Sub-sector Risk Assessment Collective Investment Sector (update 2025)*, 2025 (link)

[27] CSSF Newsletter 265 (April 2023) (link) and CSSF 2022 Annual report (link)

[28] UCIs total net assets as of 31 December 2023; data as reported in CSSF's newsletter 277 (link)

[29] CSSF, *ML/TF Sub-sector Risk Assessment Collective Investment Sector (update 2022)*, 2022 (link)

[30] CSSF, *Collective Investments Sub-Sector Risk Assessment* (page 7), 2020 (link)

[31] Corresponding to 10 EMIs and 2 branches operating in Luxembourg. 2023 data provided by CSSF.

[32] Corresponding to 15 PIs and 2 branches operating in Luxembourg. 2023 data provided by CSSF.

[35] With the adoption of the Regulation Market in Crypto Assets, VASPs operating outside Europe are required to have a presence in Europe to offer their services to the European market and be authorized as Crypto Asset Service Providers (CASP).

transactions worth EUR 22.6 billion in VAs exchanged against fiat currencies or another type of VA, administered 115,000 deposits worth EUR 4 billion in VAs and held EUR 5.9 billion of VAs in custody, while VASPs offering VAs transfer services processed transfers worth EUR 6.1 billion. In 2022, nine registered VASPs processed 16.7 million of transactions and 587,000 transfers (for VASPs offering VAs transfer services); there were 84,000 deposits and EUR 6 billion of VA held in custody.

Specialised PFSs: Luxembourg's Specialised PFS sector is large in size and carries a material risk driven by the fact that many of these professionals conduct trust and company services (TCSP) activities: out of a total of 100 Specialised PFSs supervised by the CSSF in 2023, 85 performed TCSP activities[36]. International guidance highlights how TCSP activities hold an inherently higher **PF/TF TFS risk** as they can be used to create corporate entities that designated persons and entities use to obfuscate their ties with transactions[37]. The proportion of business relationships from in-scope countries is close to zero, as is the proportion of revenue derived from in-scope countries[38].

Insurance: The primary driver of PF/TF sanctions-related risk for insurers is exposure to the maritime industry, which for Luxembourg is relatively moderate. Whilst the non-life insurance and reinsurance sectors have some exposure to the maritime industry, this only accounted in 2023 for around 6% of total turnover/premiums[39]. Notwithstanding this, the non-life insurance sector is growing and welcomed a third Protection and Indemnity (P&I) club in 2021.

Legal professions, chartered accountants, statutory auditors, and accountants: The numerous professionals belonging in Luxembourg to this sector can act as key intermediaries in financial transactions (e.g. legal entity set-up, legal advice on financial transactions, mergers & acquisitions), which exposes them indirectly to TFS-related risks. The various sub-sectors are relatively large – particularly lawyers (3,437 supervised professionals) and chartered professional accountants (1,160 supervised professionals) – and they serve a diverse, and often highly international, client base. That said, across all sectors, exposure to in-scope countries is relatively limited. **The subset of professional service providers in Luxembourg that are not self-regulating are considered to have a high inherent risk on account of the services they provide**. These operators include accounting professionals, as well as in some cases professional directors[40] and business offices: the latter two are classified as TCSPs and as described above can carry out activities that are high risk from a TFS perspective[41].

Dealers in goods: While dealing in high-value goods is typically a high-risk activity in relation to TFS, the size of the sector in Luxembourg is small and therefore exposure is relatively moderate. Globally, the anonymity and bearer-instrument nature of high value goods such as precious metals, art or luxury items make dealers vulnerable to risks related to sanctions breach, non-implementation or evasion, and recent UN Monitoring Team reports have highlighted their exploitation by actors such as ISIL and Al-Qaida[42]. However, the sector in Luxembourg is small. For example, dealers in precious metals and stones (a sub-set of the precious metals, jewelers and clocks sub-sector) consisted of 130 entities with a turnover of around €123 million at the end of 2023[43].

Freeport: Globally, freeports are inherently high risk on account of the high degree of security and confidentiality that they offer to clients and therefore their potential attractiveness for individuals seeking

[36] Data provided by CSSF for this risk assessment, 2023.

[37] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 24), 2021 (link)

[38] Data provided by CSSF for this risk assessment, 2023.

[39] For non-life insurance, marine lines represent in 2023 a turnover of €1,140.5 million, which represents 6% of the total turnover of €19.2 billion. For reinsurance, the volume of premium written for maritime, aviation and transport insurance (disaggregation is not possible) combined amounts in 2023 to €849.6 million, hence 6% only of the total volume of reinsurance premiums written.

[40] When the service provided meets the definition of article 1 (8)(b) of the 2004 AML/CFT Law.

[41] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 24), 2021 (link)

[42] UN, *Monitoring Team's Twenty-eighth report,* (page 18), 2021 (link)

[43] Data provided by AED for this risk assessment, 2021.

to disguise beneficial ownership[44]. The Freeport located in the Luxembourg Findel airport encompasses 22,000 m^2 and is designed specifically for storage of high value goods. Inflows and outflows are largely cross-border and for an international client base. In 2023, the sector had 5 authorized operators[45].

Legal persons and legal arrangements: Legal persons and legal arrangements are considered internationally as the primary vehicle for PF/TF TFS breach, non-implementation or evasion. Thus, their significant number in Luxembourg results in a very high inherent risk. As of December 2023, there were 146 373 (compared to 139,214 in 2020) legal persons registered with the Registre des Compagnies et Sociétés ("RCS"), the majority of which taking the form of *sociétés commerciales*[46]. As noted in the ML/TF Vertical Risk Assessment Legal Persons and Legal Arrangements (2022)[47], data sourced from the Registre des Bénéficiaires Effectifs ("RBE") shows that although non-residents in *sociétés commerciales* amounted to more than half of all legal persons, the BOs of the remaining types of legal persons were mostly national residents[48]. Moreover, connections with in-scope countries are limited[49]. In addition to *sociétés commerciales*, there were 8,650 Luxembourg ASBLs and *fondations* as of the end of 2021[50], although most were considered as not falling within the FATF definition of NPO and had no international dimension as per their purpose. Entities falling under the FATF definition of NPO and engaged in activities abroad are globally more vulnerable to misuse for TF purposes[51].

This report also provides a description of several **"cross-sector" vulnerabilities** in Luxembourg:

- **Virtual assets ("VAs"):** VAs are globally considered as presenting material vulnerabilities given the (pseudo-)anonymity they may offer, their international nature and high volume of transactions, the speed of execution and irreversibility of the transactions, the non-face-to-face business relationships involved and their technological complexity[52].

  Luxembourg's role as a global financial, investment and international payments centre, together with its stable regulatory framework, provides an attractive environment for new and established financial technology firms. Luxembourg has a track record of financial innovations and is committed to providing a productive and supportive environment for innovative finance businesses. While it may be not as pronounced as in some other European countries, Luxembourg's domestic market presents an appetite for VA-related services, considering the number of VASPs registered in Luxembourg.

  With the adoption by the European Union of the Markets in Crypto-Assets Regulation (MiCAR), any entity operating outside the European Union and seeking to offer its services across the European single market is required to have an establishment in one of the European Member States. In this context, Luxembourg might be selected by third-country entities to set up their European hub.

  At the international level, the global VA ecosystem has significantly grown over the last decade. The increase in number of VA and VASP types has been accompanied by more VA users, transactions and revenues. The number of VAs users worldwide has exploded from 5 million in

[44] Luxembourg, *National Risk Assessment* (page 121), 2020 (link)

[45] Data provided by ADA for this risk assessment, 2023.

[46] LBR data as of 31 December 2023.

[47] Luxembourg, *ML/TF Vertical Risk Assessment Legal Persons and Legal Arrangements,* 2022 (link)

[48] To note that as, an exception, the broad category "Other legal persons" had the highest level of non-resident BOs. This is mostly explained by the presence of non-residents in FCPs within this category.

[49] For example, based on all legal entity types, there were 53 beneficial owners that were resident of an in-scope country.

[50] Data provided by LBR.

[51] Luxembourg, *Terrorist Financing Vertical Risk Assessment*, 2022 (link)

[52] Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers,* 2020 (link)

2016 to roughly 617 million in June 2024[53,54]. As of the end of December 2023, the crypto market capitalisation reached EUR 1.66 trillion and the total crypto market volume over 24 hours amounted to EUR 64.52 billion[55].

The increased user adoption of VAs, along with their inherent technological features, have led to a significant uptake of VAs for ML/TF activities as well as potential circumvention of international financial sanctions. VAs, including anonymity enhanced coins/cryptocurrencies, are also increasingly used by terrorist financing groups such as ISIL, Al-Qaida and affiliates, and cybercriminals. Terrorist financing groups appear to have a growing affinity for stablecoins as they are less volatile. In addition, illicit VA-related activities to finance the proliferation of weapons of mass destruction pose a significant threat, mostly through theft of VAs, ransomware attacks, and the creation of fraudulent non-fungible tokens (NFTs).

Globally, several jurisdictions and international bodies have recognised the rising ML/TF threat of VAs and VASPs. The EU Supranational Risk Assessment ("SNRA") also recognised the rising risk of VAs and VASPs being misused for ML/TF purposes[56]. Furthermore and as highlighted in the FATF Targeted Update on implementation of the FATF standards on VAs and VASPs published in July 2024, many countries have explicitly analysed the vulnerability of VAs and VASPs and published correspondent risk assessments.

Finally, at the international level, links to both DPRK and Iran have been detected via the illicit use of VAs.[57] A March 2024 report on DPKR from the UN PoE indicated that 58 suspected cyberattacks by DPKR on cryptocurrency-related companies had been identified between 2017 and 2023, for a value of approximately USD 3 billion, reportedly helping to fund the country's development of weapons of mass destruction.[58]

- **Cash:** Globally, cash has been described as "a prevalent aspect of terrorist operations"[59] and has also been used by those seeking to evade PF TFS[60]. As a landlocked country in the centre of Europe, Luxembourg may be exposed to significant cross-border movements of cash (particularly for amounts below the EU declaration limit). However, relative stability in cross-border cash declarations (<1% of EU total)[61] and ATM withdrawals in-line with the broader socio-economic landscape suggest the vulnerability of Luxembourg is relatively moderate.
- **Prepaid cards:** Prepaid cards have been highlighted in FATF guidance as an important vulnerability globally, primarily in relation to TF and particularly in respect to so-called "open-loop" cards which can provide their users with a certain level of anonymity whilst facilitating cross-border transactions[62]. Globally, there is no evidence that prepaid cards are used for financing programmes of weapons of mass destruction given that the amounts for payments using prepaid cards are most of the time very small. However, it cannot be ruled out that this payment method could be used to purchase dual-use good items. Whilst Luxembourg recognised these instruments as an emerging risk in the 2018 and 2020 NRAs, the inherent exposure is relatively low. The largest issuer in Luxembourg stopped its "open-loop" cards activity and no payment or e-money institutions was issuing prepaid cards as of December

[53] Statista, *Crypto users worldwide 2016-2024*

[54] Messari Crypto, *Estimating "Real 10" Exchange Revenue*, April 2019

[55] CoinMarketCap, *Cryptocurrency Prices, Charts And Market Capitalizations*

[56] European Commission, *Supranational Risk Assessment*, October 2022 (link)

[57] RUSI, *Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia*, 2019 (link)

[58] UN, *Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)*, 2024 (link)

[59] FATF*, Emerging terrorist financing risks*, 2015 (link)

[60] FATF, *FATF guidance on counter proliferation financing*, 2018 (link)

[62] FATF, *Emerging terrorist financing risks*, 2015 (link)

2023[63]. In 2023, only one bank issued prepaid cards to their clients (which are well identified), and one known professional of the financial sector provided prepaid cards as a side-product and solely to their accountholders.

- **Social media and crowdfunding:** There is evidence globally of crowdfunding platforms being misappropriated to fund terrorist activity, or social media being used to elicit donations; as a consequence, they have been under increasing focus as a potential vulnerability[64,65]. According to a report published by the Royal United Services Institute (RUSI) in 2019, it appears that new technologies (e.g. social media and crowdfunding) have not played a predominant role in the financing of most European terrorist attacks (i.e. those performed by lone actors and small cells). In most cases, attack-related items had been previously owned by the attacker or had been procured using cash or other common banking payment methods[66]. Larger terrorist groups have globally been observed to use virtual assets, donation-based crowdfunding, social media and payment services providers, especially in the "raising" and "moving" stages[67]. Overall the report states that new technologies have been added to, rather than replaced, traditional financing methods[68]. These platforms were highlighted as a risk related to TFS evasion in the EU SNRA[69], but there are currently no major international Social Networking Services (SNS), Content Hosting Services (CHS) or Internet Communications Services (ICS) headquartered in Luxembourg. Generally speaking, a significant part of global crowdfunding uses payment methods such as bank transfers, credit/debit cards and internet payment services[70]. Luxembourg banks, PIs and EMIs offer such services to other professionals abroad. However, only one bank and one MVTS provider (which concerned only very few platforms) were offering this service as of 31 December 2023. In this context, it is also important to note that the above-mentioned MVTS provider reviewed its strategy and restricted its client base in order to concentrate on "high-quality platforms".
- **Maritime sector:** Whilst export sanctions are not in scope of this report, maritime vessels can be the subject of TFS and deceptive shipping practices can be a method of indirect TFS evasion. Despite being landlocked, the maritime fleet flying the Luxembourg flag stood at around 200 ships in 2024 and around 225 active companies were established in Luxembourg[71], potentially exposing the country to some TFS-related risks. However, the indirect exposure that results from the close links between the maritime sector globally and Luxembourg's financial and professional services sectors is more material (e.g. the risk of providing corporate services to an international vessel that is then involved in TFS breach, non-implementation or evasion).
- **Trade finance:** Trade finance is another activity that may be exploited for circumvention of sanctions and for the financing of WMD. As highlighted by the FATF and the Egmont Group in 2020, the vulnerabilities stem from the cross-border nature of the trade of goods and commodities, the involvement of multiple stakeholders and financial intermediaries which are established in multiple jurisdictions, the nature of the goods (which can be high value goods, dual-use good items...) and the amount and complexity of the transactions involved. Typical methods for misusing trade financing are the exploitation of shell and front companies, over- and under-invoicing of goods and services, over- and under-shipment of goods and services,

63 Data provided by CSSF for this risk assessment, 2023.
64 FATF, *Crowdfunding for Terrorism Financing*, October 2023 (link)
65 UN, *Midterm report of the Panel of Experts submitted pursuant to resolution 2569 (2021),* 2021 (link)
66 RUSI, *Bit by Bit*, 2022 (link)
67 RUSI, *Bit by Bit*, 2022 (link)
68 RUSI, *Bit by Bit*, 2022 (link)
69 European Commission, *Supranational risk assessment*, 2019 (link)
70 Asia/Pacific Group on Money Laundering and Middle East and North Africa FATF, *Social Media and Terrorist Financing*, 2019
71 Luxembourg, *Maritime Sector*, accessed December 2024 (link)

multiple invoicing, falsely described goods and services, fraudulent documentation and use of multiple third-party intermediaries facilitating invoice settlement. Despite the geopolitical tensions, Euromoney concluded in 2024 that an increase in the use of trade financing is expected over the next three years based on its Trade Finance Surveys[72]. An analysis made by Saenz and Lewer in 2022 identified that trade-based money laundering amounted to between USD 0.9 to 1.8 trillion within the European Union[73]. In Luxembourg, as trade finance is not an activity deeply developed by banks, the vulnerability is relatively limited.

- **Dual-use items:** Dual-use items (to be understood as including goods and technology) have both civil and military applications. By their very nature (as they can contribute to the proliferation of WMD), they are particularly exposed to PF-related risks and actors could potentially be involved at different stages of the PF value chain either directly (e.g. selling a dual-use item to a sanctioned individual/entity) or indirectly (e.g. providing financial services to a company that facilitated such a transaction). In Luxembourg, vulnerability is relatively limited as the Grand Duchy does not have a significant manufacturing industry, and its economy is orientated primarily towards financial services rather than manufacturing. Furthermore, very few export licenses have been granted in relation to higher-risk countries in scope of TFS, and none since 2018[74].

[72] Euromoney, *Trade Finance Survey Results 2024* (link)

[73] M. Saenz, J. Lewer, *Estimates of Trade Based Money Laundering within the European Union*, 2022 (link)

[74] Data provided by OCEIT for this risk assessment, 2021.

2. Introduction

This risk assessment aims to deepen the understanding of risks relating to the "breach, non-implementation or evasion"[75] of Targeted Financial Sanctions (TFS) in Luxembourg for PF and TF, imposed by United Nations Security Council resolutions (UNSCR) and EU sanctions regimes. Risks of non-compliance with such implementation are labelled as "TFS risks" throughout the report. The risk assessment also aims to identify specific areas of Luxembourg's national sanctions regime that require further strengthening.

The report follows a similar approach and methodology as other vertical risk assessments conducted in Luxembourg[76] and builds on the approach of the 2020 NRA[77].

The report consists of five main sections:

- The **stakeholders and methodology** section describes the stakeholders engaged and the approach used for this risk assessment.
- The **inherent risk - threats** section describes the threats in Luxembourg related to PF/TF TFS.
- The **inherent risk - vulnerabilities** section explores the risk factors and sectors that could render Luxembourg more susceptible to key threats. It focuses both on:
  - Sector-specific vulnerabilities: aligned with sectors in NRAs; and
  - Cross-sector vulnerabilities: analysis of cross-sectoral factors driving greater risk exposure: virtual assets, cash, prepaid cards, social media and crowdfunding, maritime sector, trade finance and dual-use items.
- The **mitigating factors** section describes the measures put in place by different public authorities, self-regulated bodies and private sector entities to mitigate the risk of sanctions breach, evasion or non-implementation.
- The **residual risk assessment** section assesses the level of residual risk for sectors analysed in the sector-specific vulnerabilities.

2.1. Introduction to proliferation financing

WMD pose a serious threat to international peace, security, and human life. Whilst nuclear warhead numbers have declined since peaking in 1986 at around 70,300 to around 13,400 in 2020, their sophistication has increased significantly since their first use in 1945[78,79]. There are indeed some cases where the use of nuclear power is entirely legitimate, such as the acquisition of materials related to the production of nuclear energy or the presence of established nuclear weapons programmes. However, for the purposes of this report, such cases are excluded, with the focus solely on illegitimate proliferation activity.

[75] FATF, *Recommendations,* Recommendation 1 (link)

[76] At the time of writing, Luxembourg's other vertical risk assessments include, amongst others, vertical risk assessments on VASPs (link), on TF (link) and on legal persons and legal arrangements (link).

[77] Luxembourg, *National Risk Assessment*, 2020 (link)

[78] Our World in Data, *Nuclear Weapons* (link); Arms Control Association (link); Federation of American Scientists, *Status of World Nuclear Forces* (link); The Nation, *The World's Most Dangerous Nuclear Weapon Just Rolled Off the Assembly Line*, 2019 (link). All pages accessed July 2025.

[79] The following countries were known in 2020 to have nuclear programmes: DPRK, China, Russia, India, Pakistan, Israel, France, UK and the USA. Note: Iran is not known to have current nuclear bomb capability. Source: Arms Control Association (link and link).

Luxembourg's Law of 27 June 2018 adopts the following definition of proliferation: *"any act contributing to the manufacture, the acquisition, … of weapons, biological or nuclear or other explosive nuclear devices and missiles that can serve as vectors for such weapons, including dual-use technologies and goods used for non-legitimate purposes, in violation of an international treaty binding the Grand Duchy of Luxemburg"*[80].

According to FATF, the financing of proliferation refers to "*the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both technologies and dual-use goods for non-legitimate purposes)*[81]".

2.1.1. Stages of the proliferation financing value chain

The complexity around the definition of PF is driven by the multiplicity of methods and types of PF. As a result, international guidance has alerted to the importance of jurisdictions understanding their exposure to risk factors along "proliferation pathways" or value chains more broadly[82]. In 2018, the Centre for a New American Security published a paper exploring the three-part PF value chain, an adapted version of which is covered in the figure below.

Figure 1: Stages of Proliferation Financing according to the Centre for New American Security[83]

1 Raising funds	2 Obscuring/moving funds	3 Using funds (procurement)
• **Goal:** Raise funds for the programme • **Examples** – State budget – Licit overseas commercial enterprises – Illicit overseas activity e.g. cybercrime	• **Goal**: disguise and transfer funds into the **international financial system** to enable proliferating activities • **Examples** – Bulk cash – Front and shell companies – Offshore companies – Accounts controlled by foreign nationals	• **Goal:** Acquire **goods, materials, technology and the logistics** required to fund its WMD programme • **Examples** – Brokers – Shipping agents – Dual use items

Stage One involves states raising money legally or illegally as part of domestic budgets and/or licit or illicit overseas activities. For example, it is estimated that the DPRK "*puts over 95% of North Korea's foreign currency earnings generated from coal exports toward the advancement of North Korea's military, nuclear missiles, and other weapons programs*"[84]. Proliferators also engage in illicit activities. For example, PF typologies have highlighted a range of illegal activities to raise funds, which include trafficking of drugs and

[80] Article 2, Law of 27 June 2018 (link)

[81] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021 (link)

[82] See for example RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment*, 2019 (link).

[83] J. Brewer, *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation, CNAS*, 2018 (link)

[84] Testimony of a North Korean defector, as reported in United States, *National Proliferation Financing Risk Assessment*, 2018 (link).

wildlife, smuggling of goods and labour exploitation[85]. One example that has received growing focus from UN Panel of Expert reports related to DPRK is the use of cybercrime. DPRK has been found to have a special "Unit 180", a cyber warfare cell within DPRK's main intelligence agency[86]. According to a North Korean defector, the hackers conduct their operation outside of DPRK, often using the guise of being employed by overseas branches of North Korean firms or trading firms[87].

Stage Two involves the transfer of funds into the international financial system. For non-sanctioned state actors, or lone actors serving a non-sanctioned state, this process is relatively straightforward. However, for states subject to sanctions (DPRK and to a lesser extent Iran), this stage is complex, as designated entities and individuals must evade or breach sanctions to access the global economy. Numerous techniques may be leveraged to obfuscate identity and BO at this stage, from use of offshore companies to accounts controlled by foreign nationals; from money remittance businesses to bulk cash[88].

One technique frequently referenced in international guidance is the use of complex networks of front and shell companies. DPRK, for instance, allegedly uses webs of front companies to disguise activities alongside associates whose ties to DPRK are hidden to conduct financial transactions[89,90]. In such cases funds often sit in foreign banks and are moved around, often never entering DPRK, and are increasingly broken into smaller amounts to reduce the chance of transactions being stopped[91]. The complexity of these corporate structures renders effective KYC and compliance processes highly challenging[92], and means that such a process can resemble something closer to a "traditional" ML scheme rather than being connected to proliferation. The sophisticated usage of shell companies also means that foreign firms may inadvertently enter into a joint venture with sanctioned states such as DPRK[93].

Stage Three involves the proliferating state or actor using funds to pay for goods, materials, technology and the logistics, which support its WMD activities. In some cases, the materials being procured involve dual-use goods[94]. These are defined by the EU Regulation 2021/821 as *"items, including software and technology, which can be used for both civil and military purposes, and includes items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices"*[95], which are subject to export controls. At this stage, financial institutions can be involved in processing the transactions[96], which – due to the obfuscation activity in Stage Two – can look like normal commercial activity and may fall below thresholds that may trigger ML-related investigations[97]. Other agents that may be involved include brokers, shipping agents, freight forwarders and the goods manufacturers themselves[98].

Across each stage of the value chain, individuals and firms may be involved directly or indirectly in PF TFS breach, non-implementation or evasion. A UK risk assessment, for instance, provides the direct example of a company providing internet banking services to a government shipping agency which allowed a state actor

85 RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment*, 2019 (link)
86 Reuters, *Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West*, 2017 (link)
87 Reuters, *Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West*, 2017 (link)
88 Cayman Islands, *Identifying Proliferation Financing* (pp. 11-21), 2020 (link)
89 Wall Street Journal (link)
90 UN, *Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020),* 2021 (link)
91 Wall Street Journal (link)
92 UN, *Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020)*, 2020 (link)
93 UN, *Final report of the Panel of Experts submitted pursuant to resolution 2464 (2019),* 2020 (link)
94 J. Brewer, *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation, CNAS*, 2018 (link)
95 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) (link)
96 J. Brewer, *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation, CNAS*, 2018 (link)
97 Cayman Islands, *Identifying Proliferation Financing*, 2020 (link)
98 Cayman Islands, *Identifying Proliferation Financing*, 2020 (link)

to import dual-use items in breach of sanctions requirements[99]. Indirect examples may include providing charity funding which is subsequently diverted to support proliferation activities[100], or Designated Non-Financial Businesses and Professions ("DNFBPs") providing services for a shell company which inadvertently legitimises its activity in a way that enables the disguising of funds.

Alongside direct and indirect links to the PF value chain, the expanding scope of sanctions regimes against DPRK means that activities covered under the scope of PF are increasingly broad. Specific measures have placed controls on financial institutions, diplomats and diplomatic missions, trade, joint ventures/cooperative entities, as well as vessels and aircraft[101]. More generally, the scope of PF is highly dependent on the types of activities used by these actors, and therefore is subject to change. For instance, if a relationship was identified that saw terrorist funds being used for proliferating activities, certain terrorist actors may be absorbed into the scope of PF regimes[102].

Luxembourg's exposure to the risk of breach, non-implementation or evasion of TFS is more likely to arise from Stage Two on movement and obscuring of funds. However, given its role as a global international financial centre, exposure to the other two stages cannot be entirely excluded. The provision of domiciliation services to a front or shell company can drive exposure to PF during the stages above for Luxembourg entities. As such, as a conservative approach, this assessment considers risk exposure to designated individuals or entities abusing Luxembourg's financial and non-financial sectors whilst keeping a full breadth of PF risk factors in mind as per above.

2.2. Introduction to terrorism financing

As noted in the TF VRA, terrorism is a real threat across Europe and countries near or neighbouring Luxembourg have been significantly affected in recent years.

Whilst the overarching outcomes of TF and PF differ, there are several similarities in how TF and PF operate.

The practical undertaking of PF often uses the same channels as terrorist financing[103] with money used ultimately to purchase goods for proliferation activities and/or enable terrorist activities. Moreover, both rely on a linear money trail (as opposed to the more circuitous money trails often observed in money laundering cases) and leverage similar methods[104].

Furthermore, their increasing complexity in the face of international scrutiny makes detection challenging. Lastly, in the context of TFS, TF and PF can often interconnect and so disrupting proliferation and its financing also ultimately supports CFT and other TFS implementation efforts.

Much like proliferation, there is no universally agreed definition of terrorism. The EU, for instance, defines terrorism as acts committed with the aim "*of i) seriously intimidating a population, or ii) unduly compelling a government or international organisation to perform or abstain from performing any act, or iii) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation*"[105].

In Luxembourg, TF is defined in Article 135-5 of the Criminal Code as the "*unlawful and wilful provision of funds, assets or goods of any nature, with the intention that they should be used or in the knowledge that*

---

[99] UK, *National Risk Assessment of Proliferation Financing* (page 5), 2021 (link)
[100] UK, *National Risk Assessment of Proliferation Financing* (page 5), 2021 (link)
[101] RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment*, 2019 (link)
[102] RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment*, 2019 (link)
[103] Council of Europe, *Financing of proliferation*, accessed July 2025 (link)
[104] Cayman Islands, *Identifying Proliferation Financing*, 2020 (link)
[105] Council Common Position 2001/931/CFSP on the application of specific measures to combat terrorism, 2021 (link)

they are to be used in order to carry out an act of terrorism, even if they have not actually been used for that purpose[106]".

This assessment considers any terrorist activity taking place across in-scope countries and known terrorist groups and follows the scope of sanctions regimes set out by the UN (and so listed in FATF Recommendation 6), as well as additional EU sanctions regimes. As such, a broad conception of terrorist actors is adopted, including International Terrorism Groups, Foreign Terrorist Fighters, Lone Actors and Small Terrorist Cells, State Sponsors of Terrorism and Corporate Terrorist Groups. In-scope countries are defined as meeting the following two criteria:

- The country already has a UN and/or EU sanctions regime in place (irrespective of whether the sanctions regime is explicitly focused on TF or not);
- The country is listed in the Top 50 nations in the Institute for Economics and Peace Global Terrorism Index[107].

In-scope countries for TF therefore include Afghanistan, Iraq, Syria, Somalia, Yemen, DRC, Mali, Libya, Central African Republic, South Sudan, Myanmar, Sudan and Iran. Further details are provided in the "Inherent risks - Threats" section of this report.

2.2.1. Stages of the TF value chain

Luxembourg's TF VRA sets out three different terrorist financing "stages", in accordance with the FATF's TF risk assessment guidance: raising, moving and using funds[108]. This is explored further in Figure 2. However, it should be noted that terrorism actors can differ from proliferation actors in their organisation, motivations, operations and activities, and use different means to raise, move and use funds.

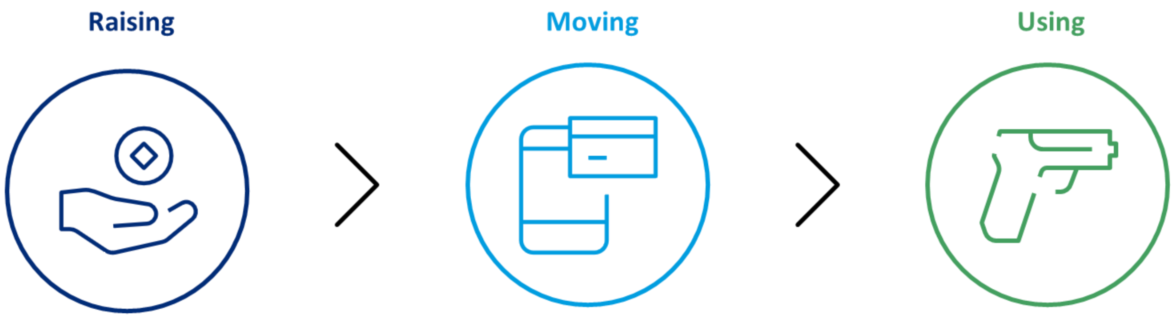
---

106 CSSF, *Fight against money laundering and counter terrorist financing*, accessed July 2025 (link)

107 Institute for Economics and Peace, *Global Terrorism Index 2023*, 2023 (link)

108 Luxembourg, *Terrorist Financing Vertical Risk Assessment* ("*Terrorism actors and their terrorist financing needs*"), 2022 (link)

Figure 2: Terrorist Financing stages[109]



Raising

- **Goal:** Raise funds intended to be used to support a terrorist or a terrorist organisation
- **Examples:**
  - Donations
  - Proceeds from organised crime activity
  - Personal savings
  - State-sponsor funds

Moving

- **Goal:** Move funds when required to finance terrorism-related activity
- **Examples:**
  - Bank wire transfers
  - MVTS services
  - Hawala
  - Cash
  - Virtual assets

Using

- **Goal:** Use funds as needed to develop intended terrorism goals
- **Examples:**
  - Administrative costs
  - Recruiting costs
  - Transportation costs
  - Weapons and materials costs

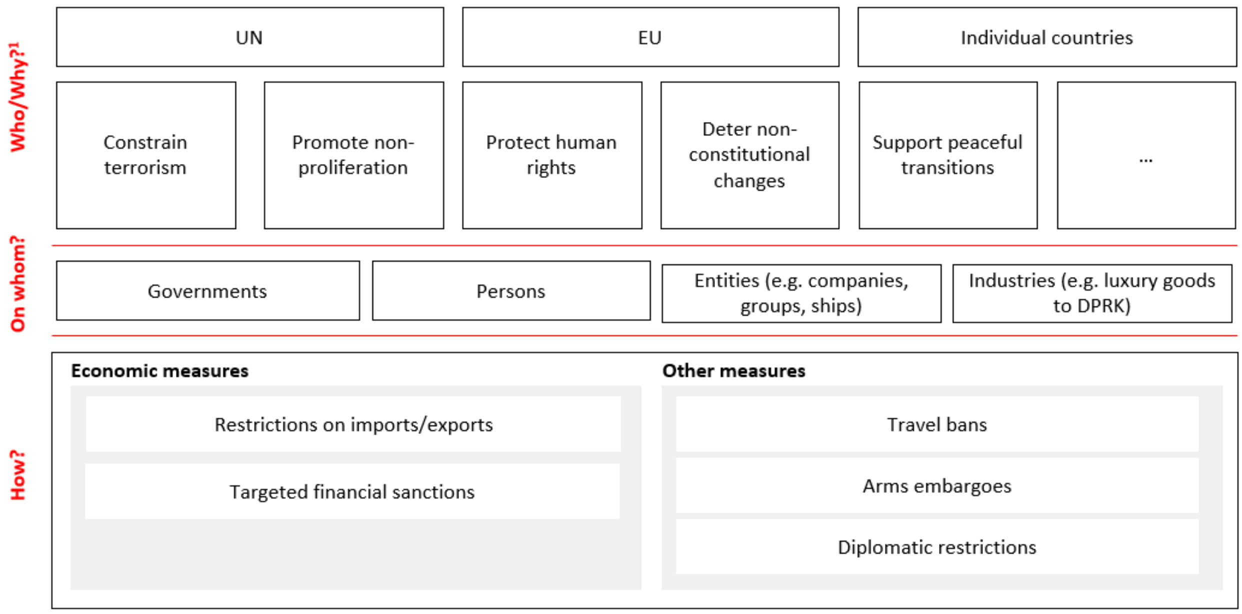
In the context of TFS, given Luxembourg's position as a financial centre with a high volume of financial flows, the exposure to the risk of breach, non-implementation or evasion of TF TFS arises mainly during the "moving funds" stage, as designated entities or persons seek to access funds illicitly in a way that evades sanctions. As sanctions related to TF and PF are increasingly applied, the methods to evade TFS have become ever more complex. More than ever, scrutiny and engagement across the public and private sectors are required to identify actors seeking to evade or breach TFS related to TF and PF.

2.3. Introduction to sanctions

Sanctions (which can also be referred to as "restrictive measures") are measures which seek to "*maintain or restore international peace and security*"[110] by restricting dealings with certain states, entities and individuals. They can be imposed by intergovernmental or supranational organisations (such as the UN or the EU) as well as governments, and their scope depends on the sanctioning authority. A group of sanctions deployed collectively is known as a sanctions regime. The overarching goals of such regimes can be broad, covering anything from addressing violations of international treaties to addressing human rights offences. They can also entail everything from travel bans and arms embargoes to comprehensive economic and trade sanctions[111]. For example, the below visualisation shows how sanctions could be deployed by the UN to counter TF across particular states, or by individual countries to tackle human rights abuses by restricting the activities of certain individuals.

[109] Luxembourg, *Terrorist Financing Vertical Risk Assessment* ("*Terrorist financing stages*"), 2022 (link)
[110] United Nations Security Council, *Sanctions*, accessed July 2025 (link)
[111] United Nations Security Council, *Sanctions*, accessed July 2025 (link)

Figure 3: Illustrative representation of different elements of a sanctions/restrictive measures regime[112]



1. 'Why' based on how the UN Security Council has applied sanctions, as listed on its website

Sanctions were first deployed by the UN in 1968 against Southern Rhodesia (now Zimbabwe). As set out in Article 41 of the UN Charter, they may include "*complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations".* Today, sanctions regimes are deployed to fulfil a range of geopolitical objectives and respond to threats to international peace and security[113]. To date, the UN has established over 30 sanctions regimes for a variety of purposes, including against Iraq, South Sudan and Mali. Fourteen sanctions regimes remain ongoing, which take different forms and pursue distinct goals, alongside broader peacekeeping, peacebuilding and peace-making strategies[114].

Beyond the UNSC, the past decade has been marked by the greater use of sanctions at a national and supranational level. For example, alongside implementing the sanctions adopted by the UNSC, the EU has increasingly used autonomous and/or incremental sanctions to fulfil certain foreign policy objectives (for example the regime against DPRK)[115]. Most sanctions adopted by the EU are targeted at individuals and entities. The EU can also adopt targeted sectoral sanctions[116]. For example, the EU Terrorist List includes individuals and organisations such as the Palestinian Hamas organisation[117].

At a national level, there has also been a trend towards greater sanctions use. For example, there was a significant increase in sanctions use by the USA during the first Trump administration, with embargoes applied regarding Venezuela, Cuba and Syria. The UK, meanwhile, has established its own autonomous sanctions regime since its exit from the EU, incorporating financial sanctions implemented by HM Treasury

---

[112] Oliver Wyman analysis, based on international reports/guidance including UN Sanctions (link), European Commission (link), Global Investigations Review (link), EU sanctions map (link).

[113] G. Martin, C. Enderby-Smith, K. Al-Faraj, *The Guide to Sanctions* in UN sanctions*, Global Investigations Review*, 2020 (link)

[114] United Nations Security Council, *Sanctions*, accessed July 2025 (link)

[115] European Council, *EU restrictive measures against North Korea*, accessed December 2025 (link)

[116] Global Investigations Review, *The Guide to Sanctions – EU Restrictive Measures*, 2021 (link)

[117] Council Decision (CFSP) 2024/332 of 16 January 2024 updating the list of persons, groups and entities covered by Common Position 2001/931/CFSP on the application of specific measures to combat terrorism, 2024 (link)

and trade sanctions and embargoes managed by the Department for International Trade[118]. The first standalone sanctions introduced in the UK since it formally left the EU in December 2020 related to the killing of Jamal Khashoggi[119]. States may also have legislative frameworks that allow them to implement unilateral sanctions. Luxembourg's legislative framework allows for the imposition of sanctions for a limited period pending the formal adoption of related decisions within the UN or the EU.

However, whilst their usage has grown, the focus of sanctions has generally narrowed to limit detrimental impacts on innocent civilians[120]. For instance, rather than very broad embargoes, measures are generally becoming more targeted, focused on particular actors and/or activities that threaten peace and stability in a sanctioned state. One key exception to this rule is DPRK, which between 2006 and 2019 was subject to nearly a dozen, increasingly expansive resolutions from the UN, as well as additional unilateral sanctions from other countries including the US[121]. Relatedly, de-risking (i.e. individuals and entities from countries under sanctions regimes being excluded from financial and business services irrespective of sanctions applying specifically to them) has also been an increasing tendency for financial and non-financial sectors that is of concern as more sanctions regimes are implemented and maintained.

Given the growing trade relationships between states, sanctions may also be cross-border and thematic in scope. The EU, for instance, has thematic sanctions including chemical weapons and cyber-attacks[122], although these are still generally less common than geographic sanctions regimes. As such, this report will focus predominantly on geographic TFS initiated by the UN and EU for the purposes of TF and PF.

2.3.1. TFS and sanctions scope for this report

The think tank Council on Foreign Relations defines economic sanctions as "*the withdrawal of customary trade and financial relations for foreign- and security-policy purposes*"[123]. They can take many forms, from comprehensive economic and trade restrictions to more targeted measures focused on specific commodities[124], business types or exports/imports.

TFS – the focus of this report – are defined by FATF as "*both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities*"[125]. Whilst sanctions are necessarily "targeted" to some extent, the key difference here is the presence of an individual/entity on a pre-defined list, with precise detail provided on the specific restrictions aimed against them. They may also be referred to as financial restrictive measures.

Supporting the implementation of TFS at a global level is among the objectives of the UN and of the FATF. Counter-PF was first introduced into the mandate of the FATF in 2012[126]. As part of Recommendation 7, countries are required to implement targeted financial sanctions to comply with UNSCRs relating to the prevention, suppression and disruption of proliferation and PF. Countries are also required to freeze without delay the funds and assets of any person (legal or natural) designated by UNSCRs and to ensure no funds are

118 Global Investigations Review, *The Guide to Sanctions - EU Restrictive Measures*, 2021 (link)
119 Global Investigations Review, *The Guide to Sanctions - EU Restrictive Measures*, 2021 (link)
120 Council on Foreign Relations, *What are Economic Sanctions*, accessed July 2025 (link)
121 Council on Foreign Relations, *What to Know about sanctions on North Korea*, accessed July 2025 (link)
122 EU Sanctions Map, accessed July 2025 (link)
123 Council on Foreign Relations, *What are economic sanctions?*, accessed July 2025 (link)
124 United Nations Security Council, *Sanctions*, accessed July 2025 (link)
125 FATF, *Targeted Financial Sanctions – International Best Practice* (page 3), 2013 (link)
126 RUSI, Guide to Conducting a National Proliferation Financing Risk Assessment, 2019 (link)

made available to that person. Immediate Outcome 11 assesses whether countries can effectively implement these obligations[127].

In addition, the importance of PF was reiterated in 2020, when FATF Recommendation 1 (focused on risk-based approach) was extended to cover PF. Moreover, Recommendation 2 was also amended in 2020 with the aim of improving the coordination of domestic efforts to combat PF. Specifically, it requires countries to implement national policies to combat PF which align with identified risks and are subject to regular review. Following the revision of the Recommendation, the FATF issued its Guidance on Proliferation Financing Risk Assessment and Mitigation in June 2021[128]. The updated Recommendation 1 also provided greater clarity on the definition of **PF risk,** which is recorded *"strictly and only"* as "*the potential breach, non-implementation or evasion of the targeted financial sanctions obligations"* (obligations mentioned in FATF Recommendation 7)[129]. To clarify, this definition does not refer to the risk of proliferation activity or the risk of PF activity, but only to the risk of non-compliance with targeted financial sanctions obligations (i.e. the risk of not meeting the requirements to apply financial sanctions to designated persons related to proliferation as mandated by the UN).

Meanwhile, FATF Recommendation 6 outlines the implementation of TFS for terrorism financing as a specific topic, alongside Immediate Outcome 10. Given the synergies of financial sanctions implementation and similarities between TF and PF, this assessment also looks at the risk of non-compliance with targeted financial sanctions obligations against terrorism financing.

Thus, this work assesses the risks associated with the potential breach, non-implementation or evasion of TFS against both PF and TF, as referenced in FATF Recommendations 1 and 2 and set out predominantly by FATF Recommendations 6 and 7 (and associated Immediate Outcomes 10 and 11). It also extends this definition to include additional EU sanctions regimes for TF, which are set out in the table below. Hereafter, "sanctions" or "TFS" refers to the UN and selected EU sanctions regimes that are in scope of this report and applicable in Luxembourg.

It is important to note that whilst the focus of this report is TFS, many of the mechanisms used for sanctions evasion are common across various types of financial and non-financial sanctions, and hence learnings can be drawn for Luxembourg's sanctions regime outside the direct scope of this report.

[127] FATF, *An effective system to combat money laundering and terrorist financing*, accessed July 2025 (link)

[128] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, 2021 (link)

[129] FATF, *Recommendations,* Recommendation 1, 2020 (link)

Table 2: Sanctions covered by this report (i.e. sanctions related to FATF Recommendations 6 and 7, plus EU and UN sanctions on in-scope countries)[130]

Country	Relevant UN Sanctions	Relevant EU Sanctions
Afghanistan (incl. the Taliban, Al-Qaida and ISIL)	Security Council resolutions 1267 (1999), 1989 (2011) and their successor resolutions, covering designations related to "*Al-Qaida, or any cell, affiliate, splinter group or derivative thereof*" Security Council resolutions 1267 (1999), 1988 (2011) and their successor resolutions, covering those "*associated with the Taliban*" Security Council resolution 2253 (2015) which expands listing criteria to include individuals and entities supporting the Islamic State in Iraq and the Levant (ISIL, also known as Da'esh). ***As listed in FATF Recommendation 6 and interpretive notes***	Council Regulation (EU) 2016/1686 imposing additional restrictive measures directed against ISIL (Da'esh) and Al-Qaida and natural and legal persons, entities or bodies associated with them Council Regulation (EU) No 753/2011 of 1 August 2011 concerning restrictive measures directed against certain individuals, groups, undertakings and entities in view of the situation in Afghanistan Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with the ISIL (Da'esh) and Al-Qaida organisations
Central African Republic	Security Council Resolution 2127 (2013), imposing an arms embargo	Council Regulation (EU) No 224/2014 of 10 March 2014 concerning Central Africa Republic
Democratic People's Republic of Korea (DPRK)	Security Council Resolutions 1718 (2006), 2087 (2013), 2094 (2013) and 2270 (2016) ***As listed in FATF Recommendation 7 and interpretive notes***	EU Restrictive Measures against North Korea (autonomous regime)) Council Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No 329/2007
Democratic Republic of the Congo	Security Council Resolution 1493 (2003) imposing an arms embargo against the DRC; Security Council Resolution 1596 (2005) imposing targeted restrictive measures; Security Council Resolution 1649 (2005) extending restrictive measures; Security Council Resolution 1698 (2006) extending restrictive measures again	Council Regulation (EU) No 1183/2005 concerning the Democratic Republic of Congo (DRC)

130 EU Sanctions Map, accessed July 2025 (link)

Country	Relevant UN Sanctions	Relevant EU Sanctions
Iran	Security Council Resolution 2231 (2015) [131] ***As listed in FATF Recommendation 7 and interpretive notes***	Council Regulation (EU) No 359/2011 concerning Iran Council Regulation (EU) No 267/2012 of 23 March 2012 concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010C Council Implementing Regulation (EU) No 2025/1548 of 25 July 2025[132]
Iraq	Security Council Resolution 1483 (2003) imposing an arms embargo; restrictions on proceeds from export sales of petroleum and gas, trade in goods, and asset freezes	Council Regulation (EC) No 1210/2003 concerning Iraq
Libya	Security Council Resolution 1970 (2011) and successor resolutions, introducing numerous restrictive measures	Council Regulation (EU) 2016/44 concerning Libya
Mali	Security Council Resolution 2374 (2017) imposing travel restrictions and an asset freeze	Council Regulation (EU) 2017/1770 concerning Mali
Myanmar (Burma)	n/a	Council Regulation (EU) No 401/2013 concerning Myanmar
Somalia	Security Council Resolution 733 (1992), imposing an arms embargo; Resolution 1844 (2008), introducing travel restrictions and an asset freeze; Resolution 1907 (2009) providing for cargo inspections; Resolution 2498 (2019) reaffirms the prohibition on certain imports	Council Regulation (EU) No 356/2010; Council Regulation (EC) No 147/2003 concerning Somalia
South Sudan	Security Council Resolution 2206 (2015) imposing various restrictive measures	Council Regulation (EU) 2015/735 concerning South Sudan
Sudan	Security Council Resolution 1556 (2004) imposing various restrictive measures	Council Regulation (EU) No 747/2014 concerning Sudan
Syria	n/a	Council Regulation (EU) No 36/2012 concerning Syria
Yemen	Security Council Resolution 2140 (2014) establishing travel restrictions and asset freezes; Security Council Resolution 2216 (2015) imposing an arms embargo	Council Regulation (EU) No 1352/2014 concerning Yemen

[131] Since 27 September 2025, all provisions of resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008) and 1929 (2010) have been re-applied in the same manner as they applied before the adoption of resolution 2231 (2015) on 20 July 2015 (link).
[132] Council of the European Union, *Timeline - EU sanctions against Iran* (link)

Country	Relevant UN Sanctions	Relevant EU Sanctions
Non-country specific	Security Council resolution 1373 (2001) covering "any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts" As listed in FATF Recommendation 6 and interpretive notes	Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP)

Countries listed in FATF Recommendations

2.4. Luxembourg's exposure to PF and TF

Luxembourg does not have a nuclear weapons programme and in recent years has not experienced any terrorist attack or terrorist group formed on its soil[133]. However, understanding potential access points or "pathways" for PF and TF that may present a higher risk exposure is vital[134]. Accordingly, this section will explore Luxembourg's exposure to potential pathways which may expose Luxembourg to PF- and TF-related TFS risks across several dimensions: geographic, trade and financial activities.

Geography: The Grand-Duchy of Luxembourg (or "Luxembourg") is a small, landlocked country but with a strategic position in the "heart of Europe". As a result, its trade and financial flows are significant for both goods and people transiting via Europe, which may increase the risk of being exposed to parts of PF and TF value chains, in particular obscuring and moving funds (as described in Figure 1). In addition, as noted in the TF VRA, Luxembourg is also in close proximity to countries which have reported a high level of terrorism-related offences. For instance, in 2023, there were 80 terrorism-related attacks (completed, failed and/or foiled) and 78 arrests in France, and 3 terrorism-related attacks (completed, failed and/or foiled) and 51 arrests in Germany[135]. This increases the likelihood of Luxembourg being used for revenue-raising activities.

Trade: Luxembourg's position in Europe makes it a significant hub for trade. In 2022, it ranked number 78 globally in total exports and 76 in total imports[136], enabled by its considerable trading infrastructure. The country has the sixth largest airfreight platform in Europe, a freeport, significant rail freight, a multimodal terminal in Bettembourg, a logistics park and a high number of lorry drivers passing through the country each day[137]. Despite being a landlocked country, Luxembourg also has a maritime industry, with more than 200 ships flying the Luxembourg flag, consisting mostly of small transporters, dredgers, tugs and supply ships[138].

STATEC data on trade in goods and services[139] shows that Luxembourg's main trade partners are EU State members and other European countries (representing in 2022 approximately 79% of exports and 90% of imports on average). Its reach is however global, including export relationships with countries in-scope of

---

[133] Europol, *European Union Terrorism Situation and Trend Report*, 2023 (link)

[134] RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment*, 2019 (link)

[135] Europol, *European Union Terrorism Situation and Trend Report*, 2024 (link)

[136] Website of the Observatory of Economic Complexity (link)

[137] Luxembourg, *2025 National Risk Assessment of Money Laundering, Observation Period: 2020-2023*, 2025 (link)

[138] Luxembourg Maritime Sector, *Luxembourg, a Maritime Alternative* (link)

[139] STATEC, *Luxembourg in figures*, 2023 (link)

this report, which are however very limited in scope (representing a value of approximately $18 million), as shown in the below table.

Table 3: Luxembourg's export relationships with in-scope countries, 2021[140]

In-scope country	Size of Luxembourg's export market (US$)	Export partner share
Afghanistan	$6,319,710	0.04%
Central African Republic	$591,870	<0.01%
Democratic Republic of Congo	$6,048,780	0.04%
DPRK	$120	< 0.01%
Islamic Republic of Iran	$929,250	0.01%
Iraq	$2,921,510	0.02%
Libya	$1,534,720	0.01%
Mali	$4,014,990	0.02%
Myanmar	$1,667,350	0.01%
Somalia	$2,200,170	0.01%
South Sudan	*Data not available*	*Data not available*
Sudan	$2,588,220	0.02%
Syrian Arab Republic	$287,080	<0.01%
Yemen	$364,140	<0.01%

Financial: Luxembourg's financial and insurance sector is the country's largest economic sector, representing 23.5% of the country's GDP during the first trimester of 2023[141]. Luxembourg acts as an EU hub and competence centre for international financial institutions. In 2023, Luxembourg's gross domestic product (GDP) at market prices amounted to EUR 79.309 billion, contributing to 0.46% of the total GDP of the EU[142]. There is a significant presence of traditional financial institutions, such as banks and investment funds, as well as technology companies that offer new and alternative payment methods. Other significant economic sectors include business activities and renting, wholesale, repair, transportation and storage, real estate activities and manufacturing. These factors can make Luxembourg entities vulnerable to exploitation by sanctioned individuals, organisations or states and therefore to breach, non-implementation or evasion of TFS obligations. As well as possible inherent exposure arising from the size of its financial sector, Luxembourg's strong reputation as a leading financial centre can make the country vulnerable to individuals seeking to legitimise their obfuscation or sanctions avoidance behaviours. In addition, whilst barriers in Luxembourg to the entry of illicit money into the EU financial system are high by global standards, once money is "in" the EU system it may be able to move relatively undetected; this trait is common to other EU member states.

[140] World Integrated Trade Solution data for 2021 (link)

[141] STATEC, *Valeur ajoutée brute aux prix de base par branche (Nace R2) (prix courants) (en millions EUR)* (link)

[142] Luxembourg, *2025 National Risk Assessment of Money Laundering, Observation Period: 2020-2023*, 2025 (link)

3. Stakeholders and Methodology

3.1. Stakeholders

The Ministry of Finance has led this Vertical Risk Assessment. The following stakeholders were also involved in the preparation of the report, including through the provision of data and analysis.

- Ministries:
  - Ministry of Foreign and European affairs, Defence, Development Cooperation and Foreign Trade (MoFA), including the Office for Export, Import and Transit Controls (OCEIT)
  - Ministry of Justice (MoJ)
- Supervisors and self-regulatory bodies (SRBs)
  - 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)
- Other stakeholders: [143]
  - Luxembourg Business Registers (LBR)
  - Administration des Douanes et Accises (ADA)
  - Cellule de Renseignement Financier (CRF)

3.2. Methodology

The methodology broadly follows that of the NRA and other vertical risk assessments conducted in Luxembourg, with some adaptations given the narrower scope of this VRA. It also references several key concepts in line with FATF guidance. These are explored further in the following table.

[143] The Banque centrale du Luxembourg (Luxembourg Central Bank or BCL) was not engaged as part of this assessment, but may be engaged for future iterations of this report.

Table 4: Key concepts for this risk assessment[144]

Concept	Definition
Threat (as per FATF)	Designated persons and entities that have previously caused or have the potential to evade, breach or exploit a failure to implement PF/TF-TFS in the past, present or future. Such threat may also be caused by those persons or entities acting for or on behalf of designated persons or entities. It can be an actual or a potential threat.
Vulnerability (as per FATF)	Matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation or evasion of PF/TF TFS.
Consequence (as per FATF)	The outcome where funds or assets are made available to designated persons and entities, which could ultimately allow them, for instance, to source the required materials, items, or systems for developing and maintaining illicit nuclear, chemical or biological weapon systems (or their means of delivery), or where frozen assets of designated persons or entities would be used without authorisation for PF and TF.
Inherent Risk (as per FATF)	The natural level of risk, prior to introducing any measures to mitigate or reduce the likelihood of an actor exploiting that risk – those measures are often referred to as controls or control measures.
Residual Risk (as per FATF)	The level of risk which remains after the risk mitigation process.

The VRA exercise is conducted in two steps. As a first step, the **inherent risk** assessment is performed by analysing threats of the potential breach, non-implementation or evasion of TFS related to TF and PF in Luxembourg across in-scope countries. It also addresses vulnerabilities, i.e. sectors' inherent vulnerability to the breach, non-implementation or evasion of TFS for PF and TF. As a second step, mitigating factors and their effects on inherent risk reduction are assessed, resulting in a **residual risk** level.

The consequences of both TF and PF are severe. WMD have the direct capacity to kill millions of people and risk harm to billions more through their secondary impacts on agriculture and the climate and the associated health outcomes[145]. Meanwhile, the significant number of deaths related to terrorism in the EU highlights the severe consequences of TF. However, there is no direct link between the amount raised/being moved and the potential consequences of its resulting activity[146] whilst, as noted by FATF in relation to PF, not all methods have equal consequences, with variations driven by the "*source, channel, or intended recipients of the funds or assets*"[147]. As a result, this risk assessment will focus predominantly on the threats and vulnerabilities of the breach, non-implementation or evasion of TFS for PF and TF.

[144] Sourced from FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 21), 2021 (link); definitions have been modified to include reference to TF for the purpose of this risk assessment.

[145] Blog of the International Committee of the Red Cross (link)

[146] United States, *National Proliferation Financing Risk Assessment*, 2018 (link)

[147] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 30), 2021 (link)

3.2.1. Inherent risk – Threats

The first step of the inherent risk assessment is an analysis of the threats facing Luxembourg. In line with the FATF definition, this risk assessment will consider the actual or potential threat of designated persons and entities having caused or having the potential to cause breach, non-implementation or evasion of TFS for PF and TF respectively.

Threats in PF risk have been segmented at a country level, in line with the UNSC Resolutions that outline targeted financial sanctions. Thus, the two types of threats are PF linked to the state of the **DPRK** and PF linked to the state of **Iran**.

Threats in TF sanction-related risk are defined as the terrorist organisations named in UNSCRs (**Al-Qaida, the Taliban and ISIL**). An additional section explores specific sanctions regimes imposed by the EU which relate to TF:

- **Afghanistan**[148]
- **Central African Republic**
- **Democratic Republic of Congo**
- **Iran**[149]
- **Iraq**
- **Libya**
- **Mali**
- **Myanmar**
- **Somalia**
- **South Sudan**
- **Sudan**
- **Syrian Arab Republic**
- **Yemen**

These additional countries were selected based on the following criteria:

- The country already has a UN and/or EU sanctions regime in place (irrespective of whether the sanctions regime is explicitly focused on TF or not); and
- The country is listed in the Top 50 nations in the Institute for Economics and Peace Global Terrorism Index (GTI)[150].

Whilst the threats analysis is separated into PF and TF, the remaining parts of the risk assessment will be treated as one analysis. This is because the vulnerabilities of sectors and controls undertaken as mitigating factors will be the same in practical terms given that the sanctions process is a uniform framework.

The countries referenced above, including DPRK, are collectively referred to as "in-scope countries" for the purpose of this report.

---

[148] Afghanistan is included for completeness but is already in-scope due to the existing UN sanctions regime.

[149] Iran is included for completeness but is already in-scope due to the existing UN sanctions regime.

[150] Institute for Economics and Peace, *Global Terrorism Index 2023*, 2023 (link)

3.2.2. Inherent risk – Vulnerabilities

The remaining part of the inherent risk assessment is the examination of vulnerabilities. The concept of vulnerability comprises matters that can be exploited by the threat or that may support or facilitate the threat. Vulnerabilities may include particular features of a sector, a financial product or a type of service that makes it directly or indirectly vulnerable to potential breach, non-implementation or evasion of targeted financial sanctions obligations.

This risk assessment takes the following approach to analysing vulnerabilities:

- First, the high-level vulnerability of each sector is assessed[151]
- Then, deep-dive analyses assess the specific Luxembourg sectors which have greater vulnerability to the breach, non-implementation and evasion of sanctions. Sectors were selected for deep-dive analyses based on FATF guidance and UN PoE reports, as well as based on their inherent exposure to ML/TF[152] as per the 2020 NRA as a corroborating factor
- In addition, cross-sector vulnerabilities are separately described, which are defined in this risk assessment as virtual assets, cash, prepaid cards, social media & crowdfunding, maritime sector, and dual-use items

The sector vulnerabilities are assessed in terms of inherent and residual risks using a "scorecard" approach (i.e. a scoring along a pre-defined set of criteria). In keeping with FATF guidance[153], the scorecard used to assess vulnerabilities is adapted from the NRA, the detail of which has been adjusted to assess PF and TF sanction-related risks. The criteria used in the scorecard have six key dimensions:

<u>Market size & structure</u>: Extent to which size and complexity of sector offer scope or likelihood for the breach, non-implementation or evasion of TFS related to PF and TF. This dimension captures the inherent exposure of a sector to sanctions threats – for example, sector fragmentation can pose greater risk, given sanctioned individuals may choose to operate through multiple or smaller firms. Compared to the NRA methodology, this dimension combines size, fragmentation and volume into one joint dimension.

<u>Ownership structure</u>: Extent to which the archetypal firm ownership model (e.g. domestic vs. international, owner type…) presents a risk of breach, non-implementation or evasion of TFS related to PF and TF. Firms that have headquarters ("HQs")/BOs in in-scope countries or in countries that are deemed higher risk or with weaker control increase the potential exposure to the breach, non-implementation or evasion of TFS related to PF and TF.

<u>Products and services</u>: Extent to which products and services (e.g. their complexity) offered by the sector allow the possibility that a breach, non-implementation or evasion of TFS related to PF and TF occurs. Certain products and sectors (e.g. trade finance) have an inherently higher risk than others; particular services may make it easier to evade sanctions, such as those that enable the formation of front and shell companies or add complexity to the value chain (in a way that disguises ultimate beneficial ownership). This dimension is targeted specifically on TFS and thus is far narrower in scope than the NRA methodology.

<u>Geography/internationality</u>: Extent to which the frequency and nature of cross-border transactions (including to in-scope countries) present risk of the breach, non-implementation or evasion of TFS. Sectors

[151] Alongside the sectors listed in the NRA, this risk assessment also includes VASPs, given their presence in the FATF's *Guidance on Proliferation Financing Risk Assessment and Mitigation*, 2021 (link).

[152] It is noted that a higher risk of ML/TF does not necessarily lead to a higher risk of PF or sanctions-related TF risk. However, certain dimensions of the NRA scorecards are relevant, such as the size and fragmentation of the sector in Luxembourg. These dimensions may generate more exposure to sanctions avoidance activities.

[153] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 21), 2021 (link)

which have a higher proportion of international business, particularly with in-scope countries or those with weaker controls, have a higher inherent risk. Note that, given the increasingly circuitous/complex nature of PF and TF value chains, any international exposure (not just with in-scope countries) can present risk. Compared to the NRA approach, this dimension aggregates two sub-dimensions: geography and flows with risky geographies.

Clients: Extent of risk posed by clients and propensity for clients to be subject to TFS related to PF and TF. It includes a consideration of factors such as the number of clients from in-scope countries and PEPs, as well as the volume of clients. Compared to the NRA approach, this dimension is much more targeted on the risk of clients being on a sanctions lists, and also aggregates two sub-dimensions: volume and risk.

Distribution channels and engagement model: Extent to which distribution methods presents risk of the breach, non-implementation or evasion of TFS obligations related to PF and TF. It includes factors such as the nature of client interaction (e.g. via intermediaries, online) and transparency and traceability of funds' movement. For example, online distribution channels can be more exposed as it can be easier to obfuscate BO/provide fraudulent documentation.

Alongside the above, there are several corroborating factors that will be used to validate the score for each sector. These will not be rated like other scorecard dimensions, but act as a useful cross-check to ensure the assigned score is aligned with expectations:

- Sanction breach, non-implementation or evasion activity observed in Luxembourg: Observed sanctions breach, non-implementation or evasion activity in various sectors in Luxembourg. The evidence of sanctions breach, non-implementation or evasion highlights its existence in a sector but also the potential efficacy of its controls, and as a result is used to corroborate rather than determine a sector's result.
- Threats exposure: Inherent exposure to common typologies of sanctions breach, evasion or non-implementation (as per international guidance and experience). This captures the degree to which common sanctions breach, non-implementation or evasion techniques are used in this sector. Given the high level of dynamism in sanctions avoidance and the need to stay vigilant to emerging risk typologies/threats, this will be used to validate the sectoral factors.
- ML and TF vulnerability: This factor captures exposure to underlying sector-specific threats of money laundering ("ML") and TF. ML risk and TF risk are distinct from PF risk. However, the consistency of some risk factors (e.g. structure & size of sector) makes this a useful "sense check" of the inherent risk result.

3.2.3. Risk scoring approach for inherent risks

Similar to the NRA approach, quantitative data and qualitative information from national and international sources are used to assess a sector's inherent risk along the criteria above (such as FATF and peer countries' risk assessments and guidance, UNSC Panel of Expert reports and academic research). Expert opinion from stakeholders (see section 3.1) is used to enrich the analysis.

The assessment is translated into a score on a scale of 1 to 5 against each criterion (1 representing the lowest and 5 representing the highest vulnerability). The generic scorecard can be found in the Appendix.

The aggregate inherent risk score for each sector is then 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", as shown in the table below.

Table 5: Inherent risk scorecard

Inherent risk rating	Risk score range
Very Low	1.00 – 1.79
Low	1.80 – 2.59
Medium	2.60 – 3.39
High	3.40 – 4.19
Very High	4.20 – 5.00

Inherent risk outcomes are reported at a sub-sector and aggregated sectoral level.

3.2.4. Mitigating factors and residual risk

In line with the NRA methodology, the risk assessment then assesses the mitigating factors, i.e. current practices and measures that contribute to combating PF risk or TF sanctions-related risk.

As with the inherent risk assessment, a combination of research, data and expert judgement from stakeholders is used to assess the impact of the mitigating factors in place along each shortlisted sector and to what extent they are able to mitigate the inherent risk level.

The impact of these internal measures is assessed against five scorecard dimensions, as listed below:

- Market entry controls: Measures undertaken by supervisors at market entry, including reviewing operators' sanctions screening processes, and treatment of any breaches
- Understanding of TF/PF risks and associated obligations: Knowledge of TF and PF pathways, as well as related typologies of sanctions avoidance, breach or non-implementation; the extent and efficacy of measures to inform sector of TF and PF risks including guidance and training
- Prevention/private sector controls: Internal controls in private sector organisations to screen against sanctions lists and implement freezes, including quality and frequency of screening, comprehensiveness of internal procedures, as well as relevant internal supporting structures
- Supervision & enforcement: Level and quality of supervisory measures and enforcement action
- Detection, reporting and outcomes: Reporting frameworks, asset freezes and outcomes reported in the sector

As with the inherent risk assessment, the impact of mitigating factors per sector is assessed using a "scorecard" approach, i.e. against a set of pre-defined criteria along each of the five dimensions above. Using the information collected and comparing against the target best practices, each sector is scored regarding mitigation on a scale from 1 to 5, with 5 representing the most significant mitigating factors. These scores are then averaged to attain an overall score, which is segmented into five possible outcomes, as the following table details. The aggregated outcomes for mitigating factors correspond to a reduction in inherent risk of 0, -0.5, -1, -1.5 and -2, respectively.

Table 6: Mitigating factors scorecard – overall impact on residual risk outcome

Mitigating factors rating	Risk score range	Impact (applied to inherent risk score)
Limited or no mitigating factors	1.00 – 1.80	0.00
Some mitigating factors	1.80 – 2.59	-0.50
Significant mitigating factors	2.60 – 3.39	-1.00
High mitigating factors	3.40 – 4.19	-1.50
Very high mitigating factors	4.20 – 5.00	-2.00

The residual risk score is assessed by combining the inherent risk score (1.00 to 5.00) with the "impact" score from the mitigating factors rating. This results in a residual risk score, per shortlisted sub-sector, which uses the same parameters as for inherent risk (i.e. as set out in Table 5).

4. Inherent Risk – Threats

4.1. TFS related to the Democratic People's Republic of Korea and to Iran

The United Nations Security Council has a two-tiered approach to countering proliferation and PF. Resolutions made under Chapter VII of the UN charter take either (1) a global approach, under UNSCR 1540 (2004, and successor resolutions), or (2) a country-specific approach, under UNSCR 1718 (2006) and the now-expired UNSCR 2231 (2015) (and successor resolutions).[154]

However, with respect to FATF Recommendation 7 on PF, TFS are involved only in the country-specific approach, that is sanctions related to the DPRK and Iran. In accordance, the threats in this risk assessment are segmented into two categories, those related to DPRK and those related to Iran.

4.1.1. Democratic People's Republic of Korea

Specific restrictions against the DPRK are listed under UNSCR 1718 (2006) and its successor resolutions. The EU framework[155] transposes these sanctions into regulations and adds further autonomous sanctions that are taken at EU level only[156]. These sanctions regimes against DPRK cover a wide range of sanction types on both individuals and entities involved in the DPRK's nuclear programme, as well as embargoes in relation to a range of imports and exports, and asset freezing (including maritime vessels)[157]. The initial sanctions under UNSCR 1718 (2006) having been expanded following DPRK's repeated violations of UN resolutions, sanctions now include the requirement to implement TFS relating to the prevention, suppression and disruption of proliferation of WMD and its financing[158].

DPRK is a prominent country in its active and intentional development of proliferation capacity. The country unilaterally withdrew from the Nuclear Non-Proliferation Treaty in 2003 and conducted its first nuclear tests in 2006, after which the UN and EU passed sanctions regimes targeting DPRK. It has conducted increasingly sophisticated nuclear tests since 2007, including a successful test of an intercontinental ballistic missile (ICBM) in 2017, and the country is known as an active exporter of ballistic missile components, technology and design data[159]. The size of the country's stockpile is unknown, though analysts estimate it could own more than 60 nuclear weapons[160]. It is believed to possess chemical weapons and biological weapons programmes[161]. Intelligence sources suggest that over 95% of DPRK's foreign country earnings are focused on the country's military, nuclear missile and weapons programmes[162].

---

154 FATF, *Guidance on Countering Proliferation Finance* (page 4), 2018 (link)

155 Council Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No 329/2007 (link)

156 Council of Europe, *EU restrictive measures against North Korea*, accessed July 2025 (link)

157 UN Security Council, *Security Council Committee established pursuant to resolution 1718 (2006)*, accessed July 2025 (link)

158 FATF, *Guidance on Countering Proliferation Finance* (page 4-5), 2018 (link)

159 Nuclear Testing Initiative, *North Korea*, accessed July 2025 (link)

160 Council on Foreign Relations, *North Korea's Military Capabilities,* accessed July 2025 (link)

161 Nuclear Testing Initiative, *North Korea*, accessed July 2025 (link)

162 US, *National Proliferation Financing Risk Assessment* (page 11), 2018 (link)

The UN sanctions regime against DPRK is designed to cut off access to any proliferation activity. TFS, which impact the financing of proliferation activity, apply to natural and legal persons designated on sanctions list for links to DPRK state-owned entities or the DPRK state. While there are broader sanctions against DPRK, for example activity-based sanctions, in 2016 the scope of UN TFS was expanded to include the following definition: "*funds, other financial resources or economics resources outside of the DPRK which are owned or controlled, directly or indirectly, by entities of the Government of the DPRK or the Worker's Party or Korea, or by persons or entities acting on their behalf or at their direction, or by entities owned or controlled by them, that the State determines are associated with the DPRK's nuclear or ballistic missile programme or other activities prohibited by relevant UNSCRs*"[163].

Following its June 2024 Plenary, the FATF reiterated its concerns over the serious threats posed by the DPRK's illicit activities related to the proliferation of weapons of mass destruction and its financing. In particular, the FATF noted that DPRK had increased connectivity with the international financial system, which raises PF risks. Therefore, the FATF called for greater vigilance and renewed implementation and enforcement of countermeasures against DPRK[164].

4.1.1.1. Methods: DPRK-specific sanctions evasion methods

DPRK has been linked to several methods that are designed to evade and circumnavigate financial sanctions, including "traditional" techniques alongside new/emerging techniques[165]. Given the large number of sanctions focused on DPRK, these methods are often highly creative and sophisticated, with elaborate schemes that might – at first sight – have no clear link to DPRK's WMD programmes[166].

In particular, DPRK has been reported to use large networks of front and shell companies, exploiting the use of complex legal structures. The state reportedly uses webs of front companies to disguise activities and uses overseas associates whose ties to DPRK are hidden to conduct financial transactions[167]. These funds can sit in foreign banks and be moved around, often never entering DPRK. They are reported to be increasingly broken into smaller quantities to reduce the chance of transactions being stopped[168]. The complexity of these corporate structures renders effective KYC and compliance processes highly challenging[169]. Meanwhile, the sophisticated usage of shell companies means that foreign firms may inadvertently enter into a joint venture with DPRK[170].

In 2017, FinCEN noted several "red flags" for these front companies and their associates[171], such as:

- **Geography:** Many of the front and shell company business addresses and/or intermediaries are registered in China or Hong Kong
- **Surge Activity Cycles:** Funds are cycled through a company for a short period of time, before lying dormant

[163] UNSCR 2270 (2016) as stated in FATF, *Guidance on Countering Proliferation Finance* (page 4), 2018 (link)
[164] FATF, *Outcomes FATF Plenary*, 26-28 June 2024 (link)
[165] FATF, Webinar on *Proliferation Financing Risk Assessment and Mitigation,* 2021 (link)
[166] US, *National Proliferation Financing Risk Assessment* (page 11), 2018 (link)
[167] UN, *Final report of the Panel of Experts submitted pursuant to resolution 2515*, 2020 (link)
[168] Wall Street Journal, *North Korea Built an Alternative Financial System Using a Shadowy Network of Traders,* 2018 (link)
[169] UN, *Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020)*, 2021 (link)
[170] UN, *Final report of the Panel of Experts submitted pursuant to resolution 2464 (2019)*, 2020 (link)
[171] FinCEN, *Advisory on North Korea's use of the International Financial System*, 2017 (link)

- **Common Front Companies:** Business lines are often stated as textile, garment, fishery and/or seafood, or may not have a stated purpose. Products and services are often unrelated to the listed business line and the company has no online presence[172]

FATF has also outlined that significant withdrawals or deposits of bulk cash are a factor linked to the DPRK regime, and a method that could be used to evade targeted financial sanctions[173].

Beyond this, DPRK has also recently expanded efforts towards cybercrime as a way of illegally accessing funds directly and so avoiding the need for elaborate TFS evasion. Several methods are used to access these funds, including cyberattacks of exchanges (which generally have weaker technology infrastructure compared to other financial institutions), social engineering and "malware exploits"[174]. Indeed, several reports have referenced the existence of a special "Unit 180", a cyber warfare cell within DPRK's main intelligence agency. According to a North Korean defector, the hackers conduct their operation outside of DPRK, often using the guise of being employed by overseas branches of North Korean firms or trading firms[175].

DPRK has also engaged in sanctions-evasion techniques related to the shipping industry, which are categorised as economic resources (and so subject to asset freezing) under UNSCR 2270 (2016)[176]. Evidence suggests that DPRK continues to operate sanctioned ships[177] and have engaged in illicit ship-to-ship (STS) transfers of cargo at sea to hide vessel identification and import refined petroleum products that contribute to the country's nuclear and ballistic missile programmes[178]. While DPRK frequently uses foreign flags on ships, vessels can be owned by trading companies or unknown parties located in other nations[179].

4.1.1.2. Threats: DPRK-related threats of sanctions evasion or breach

Given the above, the main threat to Luxembourg from DPRK designated state actors is the abuse or misuse of the financial system and/or its DNFBPs and VASPs for evading or breaching TFS. This could be by:

- Using the financial system to raise, hold or move funds to finance proliferation
- Using DNFBPs to facilitate the creation of complex legal structures
- Enabling access to bulk cash to associates of proliferation
- Misusing Luxembourg's emerging virtual assets landscape

In Luxembourg, there is no evidence to suggest that any direct associates of DPRK operate in the country or misuse its financial system directly. However, Luxembourg shares some of the factors that globally drive a threat of DPRK-related sanctions evasion or breach. As further detailed in the "Inherent risk - Vulnerabilities" section, these relate to:

- **Legal persons and legal arrangements which may be misused to create complex ownership and control structures without economic reasons** – one should note the high number of legal persons in Luxembourg (e.g. 146,373 legal persons were registered with the RCS as of December 2023)[180]. Among

[172] US, *National Proliferation Financing Risk Assessment* (page 12), 2018 (link)
[173] UNSCR 2270 (2016) as stated in FATF, *Guidance on Countering Proliferation Finance* (page 13), 2018 (link)
[174] UN, *Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020)*, 2020 (link)
[175] Reuters, *North Korea's Unit 180, the cyber warfare cell that worries the West*, 2017 (link). See also: Georgetown Security Studies Review, *DPRK Cyber Capabilities*, 2018 (link)
[176] UNSCR 2270 (2016) and UNSCR 2397 (2017) as stated in: FATF, *Guidance on Countering Proliferation Finance* (page 17), 2018 (link)
[177] UK, *UK conducts UN sanctions enforcement to counter North Korea's weapons programmes*, 2020 (link)
[178] UN, *Final report of the Panel of Experts report pursuant to resolution 1874 (2009)*, 2020 (link)
[179] Foundation for Defense of Democracies, *UN Report Reveals North Korea's Persistent and Evolving Maritime Sanctions Evasion Schemes,* 2020 (link)
[180] Data provided by LBR for this risk assessment (2023).

these, there are significant levels of foreign ownership in *sociétés commerciales* (for the remaining types of legal persons, BOs are mostly national residents)[181]

- **Large, established economy with significant flows** – which could make it difficult to monitor flows in and out of the country (both financial and trade-related flows e.g. of dual-use goods)
- **Virtual assets sector** – aspects of which were assessed as "very high" or "high" risk in the 2020 VASP VRA[182]

Jurisdictions including a port or with links to a large shipping industry and extensive shipping movements are also vulnerable to deceptive shipping practices that risk evading TFS. While shipping companies can be registered in Luxembourg, due to its landlocked location and lack of seaport this type of sanctions evasion is less of a threat. The 2020 NRA also rated Luxembourg's exposure to piracy as low[183]. That said, given its centrality to FATF guidance on PF, the maritime sector is considered as a cross-sector vulnerability in this report, and the exposure to sanctions via the insurance industry is assessed in the vulnerabilities section.

4.1.2. Islamic Republic of Iran

Specific restrictions against Iran are listed under UNSCR 2231 (2015) and its successor resolutions. These include TFS on firms and individuals linked to Iran's military and missile programs, including entities connected to the Islamic Revolutionary Guard Corps (IRGC). Whilst many sanctions remained in place, UNSCR 2231 (2015) represented a less strict regime, following international negotiation efforts in relation to Iran's nuclear programme and despite ongoing challenges[184].

Historically, after Iran's nuclear programme became public in 2002, the UNSC adopted 6 successive resolutions against the country from 2006 to 2010.[185] These aimed to pressure Iran to suspend its uranium enrichment program and undertake accompanying measures to demonstrate commitment to reducing nuclear risk. However, following international talks commencing in 2013, Iran agreed in 2015 to the Joint Comprehensive Plan of Action (JCPOA), known commonly as the "Iran nuclear deal". In this, Iran committed to reducing its stockpile of uranium and level of uranium enrichment.[186] Co-signatories of the agreement were the USA, UK, Russia, France, China and Germany, i.e. the five permanent members of the UN Security Council, and Germany (termed collectively as the "P5+1").

Following the JCPOA, UNSCR 2231 (2015) terminated many of the previous resolutions against Iran, though it retained TFS on a number of individuals and entities related to proliferation activity[187]. The EU continues to maintain several proliferation-related measures and restrictions as well as additional sanctions related to human rights (which are out of scope of this report)[188]. In subsequent years, the status of the JCPOA came into question, with the first Trump administration withdrawing from the agreement and reinstating sanctions, and Iran allegedly exceeding agreed-upon limits of uranium and methods of uranium enrichment.[189] Subsequent attempts to strengthen the JCPOA reportedly stalled and political changes in Iran

---

[181] Luxembourg, *ML/TF Vertical Risk Assessment Legal Persons and Legal Arrangements*, 2022 (link)

[182] Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers,* 2020 (link)

[183] Luxembourg, *National Risk Assessment* (page 46), 2020 (link)

[184] Since 27 September 2025, all provisions of resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008) and 1929 (2010) have been re-applied in the same manner as they applied before the adoption of resolution 2231 (2015) on 20 July 2015 (link).

[185] Nuclear Threat Initiative, *Iran*, accessed July 2025 (link); Arms Control Association, *Iran*, accessed July 2025 (link)

[186] Council for Foreign Relations, accessed July 2025 (link)

[187] FATF, *Guidance on Countering Proliferation Finance* (page 4), 2018 (link)

[188] Council of the European Union, *Timeline - EU sanctions against Iran* (link)

[189] Council for Foreign Relations, accessed July 2025 (link)

created further challenges[190]. Despite this, the EU maintained some trading presence with Iran via its "Special Purpose Vehicle" (INSTEX), which was launched by France, Germany and the UK in 2019 and aimed to support legitimate trade, focusing initially on essential sectors such as pharmaceuticals, medical devices and agri-food goods[191].

4.1.2.1. Methods: Iran-specific sanction evasion methods

Similar to DPRK, persons linked to Iran have been reported to use layers of shell companies and complex legal structures in order to move and access funds. For example, in 2019, the US Treasury took action against an Iranian bank for allegedly using a sophisticated network of front companies and agents in Iran, Turkey and the United Arab Emirates (UAE) to exchange rials for foreign currencies, a strategy that is considered to be widely employed by Iran[192]. Funds were then allegedly channelled through banks and money exchange houses in various countries using these front companies (it should however be noted that US sanctions are not in scope of this assessment).

Reports also suggest that illicit gold sales and the use of money remitters have been linked to Iran as a channel used to evade sanctions[193]. A common typology for ML/TF/PF, it is alleged that illegal gold exports and falsified food trade were features of an operation to access funds to make international payments on behalf of Iranian entities that support Iran's proliferation programme[194].

Cryptocurrency is also in development in Iran and may present an additional method of TFS evasion. In 2018, Iran declared intentions to develop a national cryptocurrency and multiple blockchain projects were presented by the central bank at a conference in 2019. Use of a cryptocurrency is reportedly being tested by Iranian banks under US sanctions, and two Iranian individuals and their bitcoin addresses were added to a US sanctions list[195]. The development of Iranian interest in cryptocurrency increases the likelihood that this method is used to evade TFS.

Across these different methods, there are several countries that have been more frequently linked to Iranian TFS evasion. For example, there have been several alleged examples related to Turkey[196] and actors in the UAE have also allegedly been linked to facilitating Iran sanction evasion. In 2020, the US Treasury Department imposed sanctions on five companies in the UAE related to this, with a Reuters investigation reporting the use of companies in Dubai and Turkey[197].

4.1.2.2. Threats: Iran-related threats of sanctions evasion or breach

Similar to DPRK, the main threat to Luxembourg from Iranian designated actors is the abuse or misuse of the financial system and/or its DNFBPs and VASPs for evading or breaching TFS. Again, there is no evidence suggesting that any direct associates of designated Iranian persons or entities operate in Luxembourg or misuse its financial system directly. However, Luxembourg shares some of the factors that globally drive a

---

[190] New York Times, *Biden Promised to Restore the Iran Nuclear Deal,* 2021 (link). See also: Arms Control Association, *JCPOA at a Glance*, 2021 (link)

[191] UK, *New mechanism to facilitate trade with Iran: joint statement,* 2019 (link)

[192] Wall Street Journal, *U.S. Targets 'Vast Network' Evading Iran Sanctions*, 2019 (link). See also: US Treasury, *Iran Sanctions*, accessed July 2025 (link)

[193] Atlantic, *The Biggest Sanctions-Evasion Scheme in Recent History*, 2018 (link)

[194] Iran Watch (published by Wisconsin Project on Nuclear Arms Control), *Major Turkish Bank Prosecuted in Unprecedented Iran Sanctions Evasion Case,* 2020 (link)

[195] Foreign Policy, *Iran has a Bitcoin strategy to Beat Trump,* 2020 (link)

[196] Financial Times, *Iranian businesses devise creative ways to evade Trump sanctions*, 2019 (link)

[197] Foundation for Defense of Democracies, *UAE Continues to Serve as Hub for Iranian Sanctions Evasion,* 2020 (link) and Reuters, *Iran scrambles to lift petrochemical sales as sanctions hammer oil*, 2019 (link)

threat of Iran-related sanctions evasion or breach. As detailed above, these relate primarily to legal entities and complex structures and the emerging virtual assets sector.

4.2. Threats in terrorism financing sanctions risks

There are two UN resolutions in scope of FATF Recommendation 6 that relate to TFS for TF:

- UNSCR 1267 (1999) and its successor resolutions apply financial sanctions to individuals and entities associated with Al-Qaida, ISIL and the Taliban.
- UNSCR 1373 (2001) requires that UN member states (i) freeze the funds and economic resources of persons who are involved in or facilitate terrorist acts and (ii) prohibit that financial services or resources be made available to such persons.

FATF Recommendation 6 requires each country to implement TFS against any person or entity designated under UNSCR 1267 (and successor resolutions) and any person or entity designated by the country under UNSCR 1373 (2001). Recommendation 6 also focuses on the preventative measures that are necessary in the context of stopping the flow of funds to terrorist groups[198].

International terrorist organisations can differ in size, structure, operational reach, motivation, recruitment and capabilities and therefore differ in the TFS threat they pose. For example, four terrorist organisations, the Taliban, ISIL, the Khorasan Chapter of the Islamic State, and Boko Haram, were together responsible for 9,223 deaths in 2018, that is approximately 58% of all terrorism-related deaths in that year[199]. However, there is no one single profile for international terrorist organisations and their financial requirements can vary significantly and are often substantial[200].

Alongside international terrorist organisations, Luxembourg's TF VRA sets out four other distinct types of terrorist actors, each of which have different financing needs:

- **Foreign terrorist fighters**: "*individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict*"[201]. Their funding needs are relatively low and come from self-funding and/or recruitment and facilitation networks[202]. Difficulty in identifying these individuals makes applying and implementing TFS challenging.
- **Lone actors and small terrorist cells**: "*The threat or use of violence by a single perpetrator (or small cell), not acting out of purely personal-material reasons, with the aim of influencing a wider audience, and who acts without any direct support in the planning, preparation and execution of the attack, and whose decision to act is not directed by any group or other individuals (although possibly inspired by others)*"[203]. They are mostly funded through small sums from legitimate activities and/or like-minded individuals. Similarly, the difficulty of identifying this diffuse set of people makes applying and implementing TFS challenging.
- **State sponsors of terrorism**: those that have "*repeatedly provided support for acts of international terrorism*"[204], by providing a so-called "safe haven" where terrorists can "*organise, plan, raise funds, communicate, recruit, train, transit, and operate in relative security because of inadequate governance*

---

198 FATF, *Recommendations*, Interpretative Note to Recommendation 6, 2020 (link)

199 Institute for Economics and Peace, *Global Terrorism Index*, 2019 (link)

200 FATF, *Emerging terrorist financing risks*, 2015 (link)

201 As defined in UNSC Resolution 2178 and quoted in Luxembourg, *Terrorist Financing Vertical Risk Assessment*, 2022 (link)

202 FATF, *Emerging terrorist financing risks*, 2015 (link)

203 RUSI, *Lone-Actor and Small Cell Terrorist Attacks: A New Front in Counter-Terrorist Finance?*, 2017. See further details on research into Lone-Actor Terrorism via this link.

204 US, *State Sponsors of Terrorism*, accessed July 2025 (link)

capacity, political will, or both"[205]. State sponsors may enable sanctions avoidance by permitting illegal flows. For instance, the Assad regime in Syria is alleged to have allowed banks in territories controlled by ISIL to continue operating[206]. Some of these state sponsors will be subject to TFS.

- **Corporate terrorist groups**: firms that sit between terrorism and organised crime, thereby having advanced and significant financing capabilities.

In keeping with the country-focused approach, this risk assessment will explore the actors named in UN Resolutions, namely Al-Qaida, ISIL and the Taliban. It will then explore TFS imposed by EU and in-scope countries selected according to the approach described in the methodology section: Iraq, Syria, Somalia, Yemen, DRC, Mali, Libya, Central African Republic, South Sudan, Myanmar and Sudan.

4.2.1. Al-Qaida, ISIL, the Taliban

Al-Qaida, ISIL and the Taliban are terrorist organisations to which specific UN financial sanctions apply. Sanctions against the Taliban were initially established under UNSCR 1267 (1999), though they were separated into a new Committee under UNSCR 1988 (2011). Al-Qaida actors were also included in lists established by UNSCR 1267 (1999) though these were then mandated under UNSCR 1989 (2011) in the Al-Qaida Sanctions Committee. In 2015, the UNSCR adopted resolution 2253 (2015) which expanded the sanctions listing criteria to include individuals and entities supporting ISIL. Furthermore, at EU level, Council Decision 2016/1693 and Council Regulation 2016/1686 impose additional restrictive measures (including TFS) against ISIL, Al-Qaida, and natural and legal persons, entities or bodies associated with them.[207]

4.2.1.1. Methods of TFS evasion

Globally, these international terrorist organisations may use a variety of methods to raise, transfer and use funds for the purpose of TF in the attempt to evade wider legal oversight including TFS. Funds are often raised through proceeds of criminal activity, such as drug trafficking, fraud and smuggling of goods. As several international terrorist organisations occupy vast territories, they may raise funds through imposing taxes and fees on local businesses, exploiting natural resources and other criminal activities[208].

Wealthy private donors making covert financial transactions can also form an important source of income for international terrorist organisations[209]. Other forms of fund raising have been developed too, with the foreign funding of international development projects securing an income flow, such as a terrorist organisation taking a funding cut from the contractor[210]. This can pose a risk to NPOs who are involved in sending donations outside of Luxembourg to development projects.

The FATF has noted that ISIL exploits the MVTS sector, especially unregistered services providers, to move funds, though it has made attempts to invest raised funds into legitimate business. For example, there may have been attempts by an ISIL network in Central Africa to establish businesses to buy gold and sell it on foreign markets[211].

[205] US, *Country Reports on Terrorism*, 2019 (link)
[206] Committee on Political Affairs and Democracy, *Funding of the terrorist group Daesh: lessons learned*, 2018 (link)
[207] European Council, *Council Decision (CFSP) 2016/1693* (as amended), 2016 (link)
[208] United Nations Office on Drugs and Crime, *Opium cultivation In Afghanistan, Latest findings and emerging threats*, 2022 (link)
[209] FATF, *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, 2015 (link)
[210] United Nations Security Council, *Letter dated 4 September 2012 from the Chair of the Security Council Committee pursuant to resolution 1988 (2011) addressed to the President of the Security Council*, 2012 (link)
[211] FATF, *FATF Actions to Identify and Disrupt ISIL, Al-Qaeda and Affiliates' Financing,* 2019 (link)

4.2.1.2. Threats related to Al-Qaida, ISIL and the Taliban sanctions evasion or breach

TFS against designated persons and entities will impact all stages of TF because raising, moving and using funds all involve financial exchanges. Luxembourg is most vulnerable to the "moving funds" stage[212] referenced in the Introduction. This is because of the country's role as a major European financial centre. Indeed, there are significant amounts of funds flowing through the country which, coupled with the high number of transactions, increases the risk exposure. More specifically and as noted in the TF VRA, the majority of terrorist attacks in countries near or neighboring Luxembourg in recent years were carried out by ISIL or by individuals who pledged allegiance to it[213].

Luxembourg has a more limited exposure to the "raising funds" and "using funds" stage. In recent years, Luxembourg has not experienced any terrorist attacks or terrorist group formed on its soil. However, the existence of an overall threat regarding those stages cannot be excluded.

The main threat in relation to designated non-state actors in international terrorist organisations is the abuse or misuse of its financial system, predominantly by the transferral of funds to international terrorist organisations in other countries and the abuse or misuse of entities falling within the FATF definition of NPO[214] for the same goal. Luxembourg shares some of the factors that drive the main threat of sanctions evasion or breach globally in relation to international financial organisations, namely:

- **Money and value transfer services (MVTS)** – which were assessed as "high" risk in the 2020 NRA and 2025 NRA and are exposed to risk of transferring funds to designated persons or entities
- **Entities falling within the FATF definition of NPO and being active in humanitarian and development aid projects abroad** – due to the fact that they may execute projects in territories that are in close proximity to terrorist organisations, with the potential for funds to be intentionally or forcibly re-routed to a terrorist organisation
- **Open borders and usage of cash** – although Luxembourg has an average usage of cash with respect to other countries of the Euro area, physical movements of cash out of, into or through the jurisdiction may be difficult to track due to open borders (it being noted that Luxembourg's vulnerability in this regard is considered as moderate – see the "Cross-Sector Vulnerabilities" sub-section for further details)

4.3. Other TF-related threats

As mentioned in the sub-section titled Methodology, several additional EU sanctions regimes are included in the scope of this report; the relevant UN and EU sanctions as well as the 2023 GTI Ranking are included below.

[212] Luxembourg, *Terrorist Financing Vertical Risk Assessment* ("Terrorist Financing stages"), 2022 (link)

[213] Luxembourg, *Terrorist Financing Vertical Risk Assessment* ("Assessing the Terrorist Financing Threat"), 2022 (link)

[214] As per the FATF's functional definition of NPO in the Interpretive Note to Recommendation 8 (link), NPO refers to "*a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works"*".

Table 7: Sanctions covered by this report, with GTI ranking (includes sanctions related to FATF Recommendations 6 and 7, plus EU and UN sanctions on in-scope countries)[215] [216]

Country	Relevant UN Sanctions	Relevant EU Sanctions	2023 GTI Ranking
Afghanistan (incl. the Taliban, Al-Qaida and ISIL)	Security Council resolutions 1267 (1999), 1989 (2011) and their successor resolutions, covering designations related to "*Al-Qaida, or any cell, affiliate, splinter group or derivative thereof*" Security Council resolutions 1267 (1999), 1988 (2011) and their successor resolutions, covering those "*associated with the Taliban*" Security Council resolution 2253 (2015) which expands listing criteria to include individuals and entities supporting the Islamic State in Iraq and the Levant (ISIL, also known as Da'esh). *As listed in FATF Recommendation 6 and interpretive notes*	Council Regulation (EU) 2016/1686 imposing additional restrictive measures directed against ISIL (Da'esh) and Al-Qaida and natural and legal persons, entities or bodies associated with them Council Regulation (EU) No 753/2011 of 1 August 2011 concerning restrictive measures directed against certain individuals, groups, undertakings and entities in view of the situation in Afghanistan	1
Central African Republic	Security Council Resolution 2127 (2013), imposing an arms embargo	Council Regulation (EU) No 224/2014 of 10 March 2014 concerning Central Africa Republic	55
Democratic People's Republic of Korea (DPRK)	Security Council Resolutions 1718 (2006), 2087 (2013), 2094 (2013) and 2270 (2016) *As listed in FATF Recommendation 7 and interpretive notes*	Council Regulation 2017/1509 concerning restrictive measures against the Democratic People's Republic of Korea	93
Democratic Republic of the Congo	Security Council Resolution 1493 (2003) imposing an arms embargo against the DRC; Security Council Resolution 1596 (2005) imposing targeted restrictive measures; Security Council Resolution 1649 (2005) extending restrictive measures; Security Council Resolution 1698 (2006) extending restrictive measures again	Council Regulation (EU) No 1183/2005 concerning the Democratic Republic of Congo (DRC)	14
Iran	Security Council Resolution 2231 (2015)[217] *As listed in FATF Recommendation 7 and interpretive notes*	Council Regulation (EU) No 359/2011 concerning Iran	21
Iraq	Security Council Resolution 1483 (2003) imposing an arms embargo; restrictions on proceeds from export sales of petroleum and gas, trade in goods, and asset freezes	Council Regulation (EC) No 1210/2003 concerning Iraq	7

[215] EU Sanctions Map, accessed July 2025 (link)

[216] Institute for Economics and Peace, *Global Terrorism Index 2023*, 2023 (link)

[217] Since 27 September 2025, all provisions of resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008) and 1929 (2010) have been re-applied in the same manner as they applied before the adoption of resolution 2231 (2015) on 20 July 2015.

Country	Relevant UN Sanctions	Relevant EU Sanctions	2023 GTI Ranking
Libya	Security Council Resolution 1970 (2011) and successor resolutions, introducing numerous restrictive measures	Council Regulation (EU) 2016/44 concerning Libya	32
Mali	Security Council Resolution 2374 (2017) imposing travel restrictions and an asset freeze	Council Regulation (EU) 2017/1770 concerning Mali	4
Myanmar (Burma)	n/a	Council Regulation (EU) No 401/2013 concerning Myanmar	9
Somalia	Security Council Resolution 733 (1992), imposing an arms embargo; Resolution 1844 (2008), introducing travel restrictions and an asset freeze; Resolution 1907 (2009) providing for cargo inspections; Resolution 2498 (2019) reaffirms the prohibition on certain imports	Council Regulation (EU) No 356/2010; Council Regulation (EC) No 147/2003 concerning Somalia	3
South Sudan	Security Council Resolution 2206 (2015) imposing various restrictive measures	Council Regulation (EU) 2015/735 concerning South Sudan	93
Sudan	Security Council Resolution 1556 (2004) imposing various restrictive measures	Council Regulation (EU) No 747/2014 concerning Sudan	93
Syria	n/a	Council Regulation (EU) No 36/2012 concerning Syria	5
Yemen	Security Council Resolution 2140 (2014) establishing travel restrictions and asset freezes; Security Council Resolution 2216 (2015) imposing an arms embargo	Council Regulation (EU) No 1352/2014 concerning Yemen	22
Non-country specific	Security Council resolution 1373 (2001) covering *“any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts”*	Council Regulation (EU) 2026/1686 imposing additional restrictive measures directed against ISIL (Da’esh) and Al-Qaeda and natural and legal persons, entities or bodies associated with them	-

“Additional” in-scope countries for this report (*compared to those listed in FATF Recommendations)*

5. Inherent Risk – Vulnerabilities

As described in the Methodology section of this report, the first stage of the vulnerability assessment involved a high-level analysis of the exposure of all (sub-)sectors analysed for the purpose of national risk assessments, based on *global* typologies for sanctions breach, non-implementation or evasion. This was to identify sub-sectors for an in-depth vulnerability analysis. FATF guidance, academic research and recent supranational and national reports on PF and TF were used to support this process. The decision to select a sector for deeper analysis is also based on the specific characteristics of this sector in Luxembourg, as set out in existing documentation (e.g. the 2020 NRA or sub-sector risk assessments). To note, the fact that a sector has been assessed as high or low risk in the 2020 NRA or in other risk assessments does not automatically translate into a high or low risk of sanctions breach, non-implementation or evasion being associated with that sector. That said, it is a useful corroborating factor, and also a source of data that can serve as reference for this risk assessment.

While, globally, some sectors are not perceived as playing a central role in the implementation of financial sanctions, it does not exclude their vulnerability to breach, non-implementation or evasion, today or in the future. The characteristics of a sanction which includes a freeze on all funds, assets and financial transactions mean that it can impact a wide assortment of organisations. Therefore, even if a sector is not selected for an in-depth analysis, it can still be vulnerable to non-compliance with financial sanctions in Luxembourg.

The table below provides a brief summary of the typical TF and PF exposure of the different sectors globally, with high-level information on these sectors in Luxembourg also included. It is followed by deep-dive analyses by shortlisted sector, with tables showing the PF and TF TFS evasion inherent risk levels at sector and sub-sector level.

Sector-specific vulnerabilities subject to deep-dive/further analysis

Table 8: High-level assessment of TFS-related PF and TF risk

Sector	Sub-sectors	Comments
Banks	Retail and business banks (including entities operating online)	• Globally, the Banking sector is considered medium risk. It is a means for designated individuals to access the international financial system[218]. • 2021 FATF guidance specifically highlights correspondent banking and trade finance as key methods used to evade sanctions[219]. • 2021 UN PoE reports have also noted the emergence of neobanks across the EU, with their weaker compliance functions, as a key mechanism exploited by ISIL and Al-Qaida[220]. • As stated in the 2020 NRA and in the 2025 NRA, Luxembourg's banking sector is exposed to ML/TF due to its size and volume of
	Wholesale, corporate and investment banks	

[218] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 23), 2021 (link)
[219] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 27), 2021 (link)
[220] UN, *Monitoring Team's Twenty-eighth report* (§70 on page 18), 2021 (link)

Sector	Sub-sectors	Comments
	Private banking Custodians and sub-custodians (including CSDs)	international business[221]. These factors also apply when considering the sector's exposure to PF and TF-TFS. • In December 2023, the sector consisted of 120 banks with a balance sheet total of EUR 929 billion and total profits before provisions and taxes of EUR 8.94 billion[222]. • Client base is international. Links with in-scope countries are limited. • Even if wholesale, corporate and investment banking services such as correspondent banking and trade finance have been identified as higher risk, trade finance is not an activity deeply developed by banks in Luxembourg and correspondent banking activities are concentrated on a few banking players.
Investment sector	Collective investments under CSSF supervision Wealth managers Brokers dealers[227] Traders/market makers[228] Regulated securitisation vehicles CSSF-supervised pension funds	• Globally, as reported by FATF, there is limited evidence of the securities industry (incl. investment sector entities) being misused or abused for financing purposes[223], although the sector is still subject to potential sanctions-related risk: – The sector is largely focused on medium to long-term asset appreciation[224] and therefore is less conducive for actors seeking to breach or evade TFS. – However, certain asset classes may be riskier from a PF/TF perspective (e.g. Private Equity and Real Assets). – Moreover, exposure may come from the higher proportion of high net-worth individuals. • In Luxembourg, the Wealth Management and Collective Investments sub-sectors have characteristics which increase their potential exposure to sanctions breach, non-implementation or evasion: – The Collective Investments sub-sector is the largest in Europe, with the sub-sector risk assessment noting it constitutes more than EUR 5,285 billion in assets under management as of 31 December 2023[225]. – As of 31 December 2023, there were 11 CSSF-supervised pension funds with EUR 1.27 billion assets under management. – As assessed in the 2020 NRA, the Wealth Managers sub-sector is characterised by substantial international business and foreign ownership[226].

[221] Luxembourg, *National Risk Assessment* (page 87), 2020 (link) and Luxembourg, *2025 National Risk Assessment of Money Laundering, Observation Period: 2020-2023*, 2025 (link)

[222] Balance sheet and profit data as of 31 December 2023; data as reported in CSSF Newsletter 279 (link).

[223] FATF, *Money Laundering and Terrorist Financing in the Securities Sector*, 2009; for PF, the sector is not referenced in the latest FATF guidance (FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation,* 2021 (link)).

[224] CSSF, *Collective Investments Sub-Sector Risk Assessment* (update 2025), 2025 (link)

[225] CSSF Newsletter 277 (link)

[226] Luxembourg, *National Risk Assessment* (page 92), 2020 (link)

[227] The term "broker dealers" herein corresponds to 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 (as per articles 24-1 and art. 24-2 of the 1993 LSF Law).

[228] The term "traders/market makers" herein corresponds to 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 (as per articles 24-3, 24-6, 24-7 of the 1993 LSF Law).

<table>
<tr><th>Sector</th><th>Sub-sectors</th><th>Comments</th></tr>
<tr><td rowspan="3">MVTS</td><td>Payment institutions (PI)</td><td rowspan="3">• Globally, MVTS providers enable cross-border transactions, which in some cases might be exploited for PF or TF:
– They enable fast and convenient transactions of multiple currencies and value, thus providing a way to fragment transactions and hide true BO.
– Given the importance of identifying BO in identifying sanctions avoidance, this puts MVTS as a higher risk sector for both PF and TF.
– Internet-based payment and e-money services have been linked to several terrorism suspects, as they enable convenient and fast low-value transactions[229] and entities that provide money remittance services can also be misused by terrorists[230].
– Unregulated and informal money transfer services, including hawala and other similar services (HOSSPs), are and continue globally to be known to be abused by international terrorist groups[231].
• In Luxembourg, the sector processes a high volume of transactions, including cross-border transactions; risk also comes from its clients, distribution model and product type.
• 29 licensed PIs/EMIs (as of 31 December 2023, including four branches of PI/EMI from another EU Member State registered in Luxembourg) processed 4 billion inflow transactions and 1.07 billion outflow transactions in 2023[232].</td></tr>
<tr><td>E-money institutions (EMI)</td></tr>
<tr><td>Agents and e-money distributors acting on behalf of PIs/EMIs established in other European Member States</td></tr>
<tr><td>VASPs</td><td>Virtual Asset Service Providers</td><td>• Eleven entities were registered as VASPs as of 31 December 2023 (including three banks, two payment institutions (PI) and one electronic money institution (EMI))[233]. In Luxembourg, the sector processes a high volume of transactions in absolute value.
• Globally, VAs are considered as possibly presenting features of material vulnerabilities given the pseudo-anonymity/anonymity they may offer, the international nature and high volume of transactions, the speed of the execution and the irreversibility of the transactions, the non-face-to-face business relationships involved, and their technological complexity.
• Globally, VASP activities might be exploited for PF or TF, where:
– the service of exchange of VA against fiat currencies serves as a bridge with the traditional financial sector;
– the service of safekeeping of VAs or instruments enabling access to VAs is exposed to cyberattacks with the aim to steal VAs;
– VAs can be transferred to a wallet belonging to sanctioned natural persons or entities through multiple actors in the chain. Once executed, the transactions are irreversible;
– The distribution model is primarily online-based.</td></tr>
</table>

[229] FATF, *Emerging terrorist financing risks*, 2015 (link)

[230] FATF, *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, 2015 (link)

[231] FATF, *Terrorist Financing Risk Assessment Guidance* (page 40), 2019 (link)

[232] Data provided by CSSF for this risk assessment, 2023.

[233] Data provided by CSSF for this risk assessment, 2023.

Sector	Sub-sectors	Comments
Specialised PFSs	Specialised PFS providing corporate services	• Globally, Specialised PFSs' provision of TCSP activities drives PF and TF TFS-related risk, as they could for example be misused for the creation of corporate entities that designated persons and entities use to obscure the links between a financial transaction and a designated person or entity[234], thereby increasing the risk of sanctions breach, non-implementation or evasion: – In Luxembourg, the size and proportion of Specialised PFS that provide TCSP services exposes the sector to risk. – Out of a total of 100 Specialised PFSs supervised by the CSSF in 2023, 85 performed TCSP activities[235].
	Professional depositaries	• Professional depositaries tailor to institutional clients from Luxembourg and abroad and provide services requiring a high level of sophistication, which limits the risk of PF and TF TFS abuse of the sector and thus the exposure to sanction breach, non-implementation or evasion.
Support PFSs & other specialised PFSs	Support PFSs	• Support PFSs and Other Specialised PFSs[236] have a low exposure to PF and TF TFS activities due to the limited client interaction and non-intervention in financial transactions: – Their activities are generally lower-risk (e.g. support services, back-office IT services, debt recovery services). – They are not likely to engage in activity related to designated persons and are less exposed to the breach, non-implementation or evasion of TFS. • In Luxembourg, they were assessed as having very low ML/TF risk in the 2020 NRA.
	Other specialised PFSs	
Market operators	Market operators	• Globally, there is relatively little evidence of the securities industry (incl. market operators) being misused or abused for terrorism or PF purposes[237]. • In Luxembourg, the PF and TF likelihood in the market operators sector is limited: – There is only one market operator in Luxembourg – the Luxembourg Stock Exchange. – While the PF and TF risks are increased due to the volume of issuance activities (EUR 1,218 billion debt value raised in 2023), the risk remains low as a limited number of institutional issuers based in low-risk jurisdictions account for the vast majority of these issuances on the Luxembourg Stock Exchange. • In Luxembourg, market operators were assessed as having low ML/TF risk in the 2020 NRA[238].

[234] FATF, *Guidance on Proliferation Financing Risk Assessment & Mitigation* (page 24), 2021 (link)

[235] Data provided by CSSF for this risk assessment.

[236] Other Specialised PFS are professionals performing lending operations (article 28-4 of the LSF), debt-recovery services providers (article 28-3 of the 1993 LSF Law), mutual savings fund administrator (article 28-7 of the 1993 LSF Law), currency exchange dealers (article 28-2 of the 1993 LSF Law) and professionals performing securities lending (article 28-5 of the 1993 LSF Law). None of the last three types of professionals are currently present in Luxembourg.

[237] FATF, *Money Laundering and Terrorist Financing in the Securities Sector*, 2009 (link); for PF, the sector is not referenced in the latest FATF guidance (FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation,* 2021 (link).

[238] Luxembourg, *National Risk Assessment* (page 13), 2020 (link)

<table>
<tr><th>Sector</th><th>Sub-sectors</th><th>Comments</th></tr>
<tr><td rowspan="6">Insurance</td><td>Life insurers</td><td rowspan="6">• Globally, although this is not as regularly referenced in international guidance, there is a potential risk that the insurance sector is exploited for TF and PF:
– For TF:
- Funds withdrawn from life insurance contracts could be used to fund terrorism[239].
- Terrorists could insure their individual risks, e.g. by registering for life insurance policies so that their families and dependents receive the pay-out post their death[240].
– For PF, a key risk area is exposure to the maritime industry[241] through the non-life and reinsurance sub-sectors:
- Some sanctioned individuals have been found to exploit insurance to facilitate the transfer of dual-use goods[242], whilst RUSI notes the importance of the insurance industry in enabling DPRK’s movement of restricted/sanctioned goods[243].
- Exposure can also be indirect (e.g. insuring ships which are subsequently engaged in ship-to-ship transfers).
• In Luxembourg, whilst the non-life insurance and reinsurance sub-sectors were both classed as low risk in the 2020 NRA[244], they still have exposure to the maritime sector.</td></tr>
<tr><td>Non-life insurers</td></tr>
<tr><td>Reinsurance</td></tr>
<tr><td>Intermediaries</td></tr>
<tr><td>PSA</td></tr>
<tr><td>CAA-supervised pension funds</td></tr>
<tr><td rowspan="5">Legal professions, chartered accountants, statutory auditors, and accountants</td><td>Lawyers</td><td rowspan="5">• Globally, legal professions, chartered accountants, statutory auditors, and accountants can act as key intermediaries in financial transactions (e.g. legal entity set-up, legal advice on financial transactions or mergers & acquisitions), which exposes them indirectly to sanctions breach, non-implementation or evasion:
– Some professionals of the legal professions, chartered accountants, statutory auditors, and accountants sector can carry out TCSP activities, which are flagged as higher-risk by FATF[245] as they enable the obfuscation of BO.
– UN PoE reports also highlight the use of false documentation to set up client accounts with TCSPs (mainly business registry services) and thus avoidance of being flagged as designated entities for sanctions[246].
– Professionals of the legal professions, chartered accountants, statutory auditors, and accountants sector may also be</td></tr>
<tr><td>Notaries</td></tr>
<tr><td>Bailiffs</td></tr>
<tr><td>(Approved) statutory auditors and (approved) audit firms</td></tr>
<tr><td>Chartered professional accountants</td></tr>
</table>

[239] IAIS, *Application Paper on Combating Money Laundering and Terrorist Financing*, 2021 (link)
[240] European Commission, Commission staff working document accompanying the document *Supranational Risk Assessment,* July 2019 (link)
[241] FATF, *Complex Proliferation Financing and Sanctions Evasion Schemes* (pages 46-53), 2025 (link)
[242] Gibraltar Financial Intelligence Unit, *Guidance Notes on Counter-Proliferation Financing*, 2020 (link)
[243] RUSI, *Underwriting Proliferation: Sanctions Evasion, Proliferation Finance and the Insurance Industry* (page vii), 2018 (link)
[244] Luxembourg, *National Risk Assessment* (page 85), 2020 (link)
[245] FATF, *Guidance on Proliferation Financing Risk Assessment & Mitigation* (page 24), 2021 (link)
[246] UN, *Midterm report of the Panel of Expert submitted pursuant to resolution 2464 (2019)* (page 22), 2019 (link)

Sector	Sub-sectors	Comments
	Accounting professionals TCSPs – professional directors TCSPs – business offices	indirectly engaged in PF or TF activity by inadvertently providing services to sanctioned individuals. • Several factors increase the exposure of professionals in this sector to sanctions-related risk, including: – The sizeable and fragmented landscape of professionals authorised to act as TCSPs. – The size, diversity and international nature of Luxembourg's financial system and legal entities and arrangements landscape, to which the professionals in this sector provide services. • For the purposes of this report, bailiffs are excluded given their relatively small number in Luxembourg, as noted in the 2020 NRA[247].
Gambling service providers	Casino Sports betting Ad hoc lotteries National Lottery Online gambling	• Globally, gambling service providers have rarely been observed to be abused for PF or TF purposes[248]. It also does not hold funds of individuals, so is unlikely to be vulnerable to sanctions-related risk. • In Luxembourg, exposure to PF and TF risk is limited, as the gambling sector is limited and mostly concentrated around two service providers: one casino and the National Lottery.
Real estate agents and developers	Real estate agents (*agents immobiliers*) Real estate developers (*promoteurs immobiliers*)	• Globally, whilst the real estate sector is considered high risk for ML[249], it is not addressed in PF or TF-specific guidance or flagged as a high-risk sector for sanctions evasion[250]. • In Luxembourg, the real estate sector is sizeable and fragmented, with a high volume and value of transactions, but mostly serves Luxembourg residents – thus the likelihood of sanctions for PF and TF is lower, with an accordingly lower risk of sanction breach: – There were 2,528 agents in the sector in 2023[251]. – In 2019, the sector reported a turnover of €899 million, with 352 agents accounting for 84% of turnover[252]. – A sample of 1,075 real estate professionals in 2021 suggests that 90% of clients are Luxembourgish residents[253].
Dealers in high value goods	Art/antiques Luxury goods	• Goods provide an alternative method for designated persons and entities to illicitly move financial resources across international borders whilst preserving anonymity, with the FATF flagging dealers in precious metals and stones as particularly vulnerable to PF[254].

[247] Luxembourg, *National Risk Assessment* (page 115), 2020 (link)
[248] FATF, *Vulnerabilities of casinos and gaming sector*, 2009 (link)
[249] Luxembourg, *National Risk Assessment*, 2025 (link)
[250] FATF guidance dated 2021 does not reference real estate (FATF, *Guidance on Proliferation Financing Risk Assessment & Mitigation*, 2021 (link).
[251] Luxembourg, *National Risk Assessment* (page 111), 2025
[252] Data provided by the AED for this risk assessment, 2021.
[253] Data provided by the AED for this risk assessment, 2021.
[254] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigating* (page 24), 2021 (link)

Sector	Sub-sectors	Comments
	Precious metals, jewelers and clocks	• Terrorist groups such as ISIL are known to exploit local resources in areas under their control, including gold, as a direct source of funds[255]. UN reports, for example, note that artisanal gold is being exploited, as customs officials lack the tools to monitor its trade [256], and so it may raise income in a way that circumnavigates TFS. • Whilst the sub-sectors are relatively small in Luxembourg, their reference in international guidance suggests they are still exposed to sanctions-related risk.
	Car dealers	
Freeport	Freeport operators	• Globally, freeports have been known to enable a high degree of security and confidentiality to clients, which might make them targets for individuals seeking to disguise beneficial ownership[257]. In other countries, freeport operators have also been abused to hide smuggled goods (e.g. alcohol and tobacco) by persons linked to terrorist organisations[258]. • While key risk drivers for ML/TF remain the nature of the Luxembourg Freeport's activities and the international nature of inflows and outflows, it should be noted that freeport operators in Luxembourg must identify the BO of the goods brought by their clients. Clients cannot use offshore companies, trusts, lawyers, nominees or galleries to shield their ownership. This makes the Luxembourg Freeport less attractive for criminals.
Legal persons and legal arrangements	Domestic "fiducies"	• Globally, legal persons and legal arrangements are commonly regarded as being highly vulnerable to PF and TF crimes: – As the OECD observes, "almost every economic crime involves the misuse of corporate vehicles" [259] since they might help conceal the origin of funds or allow funds to be moved overseas. – Designated persons linked to PF using opaque ownership structures is a common PF typology[260], thus increasing the risk of sanction evasion in this area. – Entities falling within the FATF definition of NPOs are globally considered to be more vulnerable to TF, and the FATF published a separate report in 2014 identifying five common typologies of NPO[261] misuse and abuse for TF purposes, two of which being connected to financing and hence driving exposure to sanctions evasion. • The number of legal persons and legal arrangements in Luxembourg exposes the sector to sanctions-related risk: – As of 31 December 2023, there were 146,373 (compared to 139,214 in 2020) legal persons registered with the RCS, the majority of which took the form of sociétés commerciales.
	Foreign trusts	
	Sociétés commerciales	
	Sociétés civiles	
	ASBLs and *fondations* falling under FATF NPO definition engaged in activities abroad	

[255] FATF, *Terrorist Financing Risk Assessment Guidance* (page 40), 2019 (link)
[256] UN, *Monitoring Team's Twenty-eighth report* (page 18), 2021 (link)
[257] Luxembourg, *National Risk Assessment* (page 121), 2020 (link)
[258] FATF, *Money Laundering vulnerabilities of Free Trade Zones*, 2010 (link)
[259] As reported in Luxembourg, *National Risk Assessment* (page 123), 2020 (link); original source: OECD, *Behind the corporate veil: using corporate entities for illicit purposes,* 2001
[260] FATF, *Guidance on Counter Proliferation Financing*, 2018 (link)
[261] FATF, *Risk of terrorist abuse in non-profit organisations*, 2014 (link)

Sector	Sub-sectors	Comments
	ASBLs and *fondations* falling under FATF NPO definition with local activities	– The 2020 NRA assigned a very high inherent risk rating to foreign trusts (although the specific risk was rather high for some forms of sociétés commerciales and medium and low for the rest)[262]. The LPs/LAs VRA assessed the corporate risk of ASBLs as medium (corporate risk) and high (specific risk) and the risk of fondations as high (for both corporate and specific risk). For ASBLs and fondations, the specific risk ratings in this assessment apply to those operating abroad and falling within the FATF definition of NPO [263], since these are the ones exposed to a comparatively higher TFS-related TF and PF risk.
	Other legal persons	

5.1. Banking

Sector	Inherent risk	Sub-sectors	Inherent risk
Banks	**Medium**	Retail & business banking (including entities operating online)	**Medium**
		Wholesale, corporate & investment banking	**High**
		Private banking	**Medium**
		Custodians and sub-custodians (including CSDs)	**Medium**

Given its centrality to the international financial system, globally, the banking sector is inherently exposed to illicit financial flows and risks of breach, non-implementation or evasion of sanctions. It is consistently referenced in international guidance, with a significant number of penalties issued against global banks for breach, non-implementation or evasion of targeted financial sanctions. For example, entities belonging to the UniCredit group were fined $1.3 billion in 2019 for processing $393 million through the US financial system on behalf of an Iranian entity designated as a Weapons of Mass Destruction proliferator[264].

Designated entities and/or persons[265] may use several methods to engage in PF and/or TF sanctions evasion through the banking system. The main goal being the obfuscation of money flows and of the beneficiaries of transactions, risk factors include bank accounts opened by front/shell companies[266], correspondent banking relationships, but also products related to trade finance or targeted towards the maritime industry. Other risk factors related to banking include the provision of products/services that may reduce transparency/client visibility, including TCSP or virtual asset activities[267]. The high volume of transactions that flow through bank accounts on a daily basis contributes to the difficulties of identifying transactions that might be related to PF or TF sanctions and of carrying out sufficient due diligence on parties involved in the transactions to ensure that PF or TF is not taking place.

[262] Luxembourg, *National Risk Assessment*, 2020 (link)
[263] Luxembourg, *ML/TF Vertical Risk Assessment Legal Persons and Legal Arrangements,* 2022 (link)
[264] Compliance Week, *UniCredit Group Banks to pay $1.3B for sanctions violations,* 2019 (link)
[265] Defined as persons or entities subject to TFS for PF or TF – for additional detail on in-scope sanctions programmes, see "Introduction".
[266] United States, *Proliferation Financing National Risk Assessment*, 2018 (link)
[267] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, 2018 (link)

Correspondent banking is a key risk area for both TF and PF evasion risk, given the inherent ability for respondent banks to obfuscate the beneficial owner of funds[268]. For example, international terrorist organisations such as ISIL have been observed to take control of bank branches located in their territories, which could allow them to connect to the international financial system and collect or send funds via accounts at correspondent banks[269].

For correspondent banking, UN PoE reports on PF have also highlighted the use of facilitators in Asia and the Middle East who carry out transactions on behalf of designated entities[270]. There are also instances of several intermediary financial institutions or companies in other jurisdictions being used to conduct business, resulting in the correspondent bank having limited insight on the BO or respective transactions.

Trade finance has also been identified as an activity that is more exposed to sanctions-related risks[271]. Although banks may have insight in trade finance transactions, designated persons and entities have been known to use forged documents to mask the true purpose of a transaction, the underlying customer and the nature, origin or destination of goods involved[272].

In Luxembourg, the banking sector is exposed to PF/TF sanctions-related risk, predominantly due to its international clientele, the products and services it offers and its distribution model. As of 31 December 2023, there were 120 banks in Luxembourg, with a balance sheet total of €929 billion and a net profit of €8.942 billion[273]. The sector employed 26,254[274] people as of the same date.

Banks in Luxembourg typically are subsidiaries or branches of European or international banking and finance groups. Shareholders and beneficial owners of banks are identified during the licensing process and later on when changes occur or as part of a qualifying holding assessment. As of December 2023, none of the 120 banks had UBOs from, nor branches in, an in-scope country.

In Luxembourg, most banks have a mixed business model (for example, combining retail banking, private banking and corporate banking activities), reflecting the fact that the Luxembourg banking license is a universal licence. Some Luxembourg banks carry out activities presenting higher risk for TF/PF sanctions evasion and therefore may be more exposed to PF/TF sanctions-related risks. No VOSTRO account[275] opened with a Luxembourg bank was held by a respondent bank established in an in-scope country.

The vulnerability to PF/TFS of the correspondent banking sector in Luxembourg is mostly concentrated within a small number of credit institutions. A handful of correspondent banks in Luxembourg hold more than 85% of all the correspondent banking relationships, have an international exposure and are subject to a high inherent risk. The remaining entities offer correspondent banking services to entities of the same banking group or mostly to local credit institutions.

The vulnerability to PF/TFS of the trade finance sector in Luxembourg is also concentrated within a small number of credit institutions. Only a low share of the credit institutions declares this activity as their main activity and among those a still smaller number declares it as a regular activity. These entities have international exposure and offer a wide range of services. The remaining entities are mainly involved in trade finance through participating to syndicated loans.

---

[268] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation,* 2021 (link)

[269] FATF, *Financing of the terrorist organisation of Islamic State in Iraq and the Levant (ISIL)*, 2015 (link)

[270] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 27), 2021 (link)

[271] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 27), 2021 (link)

[272] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation,* 2021 (link)

[273] Balance sheet and profit data as of 31 December 2023; data as reported in CSSF's newsletter 279 (link)

[274] CSSF Newsletter 279 (page 23), 2024 (link)

[275] A VOSTRO account in this case is a bank account held by a foreign bank with a Luxembourg bank.

Some banks in Luxembourg also perform TCSP services or report in their annual responses to the CSSF's questionnaire on financial crime having clients that are active in the virtual currency ecosystem, which are considered higher risk due to their ability to facilitate anonymity and therefore potentially the obfuscation of BO.

Luxembourg banks are also exposed due to the sector's international nature, client types and therefore cross-border flows. Whilst this still concerns a very limited proportion of total flows, some assets are reported as being related to natural persons, legal persons, BOs and PEPs with connections to in-scope countries.

The following sections highlight the banking activities that have been assessed as likely to be targeted by entities active in proliferation and thus to present a higher PF risk. It has to be reminded that most Luxembourg banks have a mixed business model and therefore may be addressed across multiple sections below.

5.1.1. Retail and business banking (including entities operating online)

Retail and business banking in Luxembourg is moderately exposed to the risk of non-implementation, breach or evasion of sanctions, predominantly driven by its very high number of clients and its distribution model.

The sub-sector of retail and business banking in Luxembourg was as of 31 December 2023 highly concentrated on a few entities. Whilst UN PoE reports have highlighted new/emerging threats[276] related to "neobanks"[277], there are currently no neobanks licensed in Luxembourg and so this risk factor does not impact the level of risk.

In terms of products and services, as of December 2023, only a handful of entities from the sub-sector offered trade finance transactions and correspondent banking services to respondent banks. Whilst no VOSTRO accounts opened with Luxembourg banks were held by respondent banks established in an in-scope country (about 12% of the VOSTRO accounts concerned are held by respondent banks established outside of the EU), transactions may still concern clients/counterparties of the respondent bank who may be directly or indirectly linked to TFS, thus entailing a slight degree of risk.

Finally, even standard services such as ATM withdrawals, which could facilitate the cross-border transfer of cash[278], are contributing to the sub-sector's TF/PF sanctions risk. In total, for all Luxembourg banks, the Banque Centrale de Luxembourg ("BCL") reported ATM withdrawals of approximately €3.821 billion worldwide with Luxembourg issued credit and debit cards in 2023 (compared to approximately €3.355 billion in 2020)[279]. While ATM withdrawals have been steadily increasing, this appears in line with the overall growth of the Luxembourg economy, its population, commuting workforce and international clientele, as well as banks' decisions to reduce the number of branches and outlets and introduce handling fees for all withdrawals conducted with staff at bank counters.

[276] UNSCR member states have noted that their less effective sanctions-screening capabilities has enabled the transfer of large sums in support of ISIL and Al-Qaida.

[277] Defined by Forbes as "*fintech firms that offer apps, software and other technologies to streamline mobile and online banking*". They are also often referred to as "challenger banks" (link).

[278] RUSI, *Guide to conducting a national proliferation financing risk assessment*, 2019 (link)

[279] Luxembourg, *2025 National Risk Assessment of Money Laundering, Observation Period: 2020-2023*, 2025 (link)

Retail and business banking entities in Luxembourg process a large volume of high-speed international transactions. A limited share of these relate to "higher-risk" countries[280] (less than 1% of total transfers). Note that this includes countries deemed "higher risk" for different compliance-related reasons and not only for reasons related to PF/TF sanctions. In addition to transactions processed by these "traditional" retail banks, there are also market participants in Luxembourg (such as payment institutions) that conduct activities that are similar to (though not exactly the same as) retail banking and have high numbers of clients and high transaction values and volumes. Given that their activities are not strictly that of "retail banks", these are not captured in the aggregated statistics of this report, but the inherent risk associated with them is reflected in the risk ratings. Like traditional retail banks, these participants are subject to supervision by CSSF (see "Mitigating Factors" section for further detail).

5.1.2. Wholesale, corporate and investment banking

The wholesale, corporate and investment banking sub-sector presents a high risk of sanctions breach, non-implementation or evasion that is driven by its product suite, its clients and its distribution model.

About 25% of the entities of the banking sector offer trade finance or correspondent banking services. Whilst no VOSTRO accounts opened with Luxembourg banks were held by respondent banks established in in-scope countries, and about 12% were established outside of the EU, this does not wholly diminish the risk, as transactions may concern clients/counterparties of the respondent bank who may be directly or indirectly linked to TFS.

In Luxembourg, the vulnerability to PF/TFS of the correspondent banking sector is mostly concentrated on a small number of credit institutions within this sub-sector. A handful of correspondent banks in Luxembourg hold more than 85% of all the correspondent banking relationships, have an international exposure and are subject to a high inherent risk.

In Luxembourg, the vulnerability to PF/TFS of the trade finance sector is also mostly concentrated within a small number of credit institutions within this sub-sector. These entities have international exposure and offer a wide range of services. The remaining entities are mainly involved in trade finance through participation in syndicated loans.

Clients may also increase risk exposure due to their geographical origin or the international nature of their business.

As concerns payment flows, less than 1% of the total incoming and outgoing payments recorded for the sub-sector during 2023 were in relation to higher risk countries based on the internal risk assessment of CSSF. Whilst this included entities deemed "higher risk" for all financial crime, the scale of the transactions linked to countries that may have weaker controls for AML/CFT in general (and thus also potentially for PF/TF sanctions risk) presents some risk to Luxembourg.

[280] This refers to the banks' own definition of higher-risk countries for AML/CFT in general, and so it is not possible to say whether this includes all in-scope countries for TF/PF sanctions-related risk.

5.1.3. Private banking

Luxembourg's private banking sub-sector is moderately exposed to risks of sanctions breach, non-implementation or evasion. The risk factor driver is the exposure to higher-risk clients.

There is a moderate level of risk associated with private banks' product suite, which is targeted primarily at long term investments by high-net-worth ("HNW") and ultra-high-net-worth ("UHNW") individual clients with higher investment amounts. However, a low share of the sub-sector's entities also offers trade finance transactions and less than 25% of the sub-sector's entities offer correspondent banking services as an ancillary activity. No VOSTRO accounts opened with Luxembourg banks were held by respondent banks established in an in-scope country, but as 57% were established outside of the EU this does not eliminate the risk, as transactions may concern clients/counterparties of the respondent bank who may be directly or indirectly linked to TFS.

The private banking sub-sector is highly international and has increasingly been serving HNW and UHNW clients, including from remote jurisdictions, which increases inherent risk. As noted in the 2022 KPMG/ABBL report "Clarity on performance of Luxembourg private banks"[281], less than a quarter of the sub-sector's Assets under Management ("AuM") in 2022 came from Luxembourg resident account holders (19%) while 63% came from account holders located within the EU (22% from neighbouring countries and 41% from other European countries), with the remaining 18% corresponding to the "Rest of the world". That said, relationships tend to be longer-term than other banking services, which may make it easier to discern unusual activity.

Lastly, the private banking sector traditionally works with business introducers, some of which may be licensed entities of the same group while others may be non-affiliated companies or individuals working with the bank on a contractual basis. While banks typically perform their own due diligence, intermediaries interacting between the bank and the client could nevertheless decrease the transparency of a relationship.

5.1.4. Custodians and sub-custodians

Overall, custodians and sub-custodians face a moderate risk of sanctions breach, non-implementation or evasion. In Luxembourg, the sub-sector is of the same size than the wholesale, corporate and investment banking sub-sector in terms of number of entities. Whilst the product suite of these entities is more standardized, with a focus on securities custody, there have been cases where intermediaries were used to avoid economic and financial sanctions through omnibus accounts[282]. The volume of assets and the internationality of the sub-sector also create some exposure[283].

A driver of product risk is the presence of intermediary accounts, which are typically used at custodians holding accounts on behalf of other professionals, such as asset managers, investment funds, insurance companies, etc.

Custodians/sub-custodians have a high share of international business and some types of clients from higher risk sectors.

---

[281] KPMG and ABBL, *KPMG-ABBL Private Banking Report, Clarity on performance of Luxembourg private banks*, 2023 (link)

[282] International Securities Services Association, *Study on the Benefits and Costs of Securities Accounting Systems*, 2015 (link)

[283] Entities delivering depositary services to investment funds are not described in this section, but in the sub-sector focused on collective investments.

5.2. Investment sector

Sector	Inherent risk	Sub-sectors	Inherent risk
Investment sector	**Medium**	Collective investments[284]	**Medium**
		Wealth managers (*gérants de fortune*)	**Medium**

5.2.1. Collective investments

Globally, the collective investments sub-sector is moderately vulnerable to risks related to breach, non-implementation or evasion of PF and TF TFS. On the one hand, much of this sector is largely focused on medium to long-term asset appreciation, which does not align with objectives to move funds easily and quickly to enable proliferation or terrorist activities. On the other hand, the cross-border distribution nature of Luxembourg collective investment funds coupled with certain types of investment strategies (e.g. real assets) can cause the sector to be comparatively more exposed to PF and TF risks.

In Luxembourg, the collective investments sub-sector has characteristics which present a potentially moderate exposure to sanctions breach, non-implementation or evasion, driven primarily by its size and distribution model. As noted in the sub-sector risk assessment, Luxembourg's collective investment sector is the largest in Europe[285]. This size and its fragmentation make the sub-sector vulnerable to being potentially abused or misused by designated individuals or entities seeking to access large amounts of funds to enable PF and TF activities.

The cross-border nature of Luxembourg collective investments sector entails a higher risk in terms of distribution. By distributing investment funds to foreign investors, the likelihood of having investors subject to TFS increases. As shown by latest data available and the CSSF's methodology to identify PF and TF in-scope countries, the distribution of CSSF-supervised funds marketed in in-scope countries is extremely limited[286], which reduces the likelihood of designated individuals from in-scope countries investing in Luxembourg funds.

Luxembourg's exposure is also tied by the types of investment products offered. There are two main categories of collective investments available in Luxembourg: UCITS and AIF. In general, AIFs present a higher risk in terms of product type, as they target investment classes which could be riskier from a PF/TF perspective (notably private equity and real assets). However, these types of investment strategies only constitute a small proportion of the sub-sector's assets under management.

5.2.2. Wealth management

As with the collective investments sub-sector, **the vulnerability of the wealth management sub-sector is limited in PF and TF sanctions-related risk**, largely due to its focus on medium to long-term asset

[284] Investment funds and managers supervised for AML/CFT purposes by the CSSF. Other types of entities supervised by CSSF are excluded from this table as they were not subject to a deep dive for this risk assessment.

[285] CSSF, *Collective Investments Sub-Sector Risk Assessment* (page 7), 2022 (link)

[286] The distribution of Luxembourg investment funds to in-scope countries represented in 2023 less than 0.003% of the total AuM. This figure may be subject to reporting errors.

appreciation which is less conducive for actors seeking to breach or evade TFS. However, as wealth managers typically cater to HNW individuals, **there is a risk of exposure to international actors linked to proliferation or terrorism**. For example, according to the 9/11 Commission Report, a group of wealthy donors from the Gulf known as the "Golden Chain" supported mujahideen with finances, including mujahideen under the leadership of Usama Bin Laden[287], who was a UN sanctioned person up until 2013[288].

In Luxembourg, the sub-sector of wealth managers encompasses "private portfolio managers"[289] (article 24-4 of the law of 5 April 1993 on the financial sector ("1993 LSF Law")) and "investment advisers" (article 24-5 of the 1993 LSF Law). Overall, it has a medium risk of sanctions evasion.

The sub-sector is medium in size and fragmentation, and relatively small compared to Luxembourg's banking sector and collective investments sub-sector. That said, **it still manages a significant volume of assets and a significant number of clients**, which increases the potential exposure to the risk of sanction breach, non-implementation or evasion. In total, 71 investment firms provided asset and wealth management services as of 31 December 2023.

There is limited geographic risk associated with wealth managers. Approximately 25% of firms have foreign non-EU ownership (the main non-EU countries being Switzerland, USA and Monaco), but no entities have a BO or parent from an in-scope country. Applicable regulations clearly prohibit opaque ownership structures. Some ownership structures that were authorised historically may have more complex structures; however, the rationale behind the set-up is understood. Tax compliance of shareholding structures is assessed by a CSSF in-house expert (the same as for other CSSF-supervised entities).

Based on the annual Financial Crime Survey, there were as of 31 December 2023 only two investment firms which held relationships related to in-scope countries (e.g. a client account opened in the name of an individual who is a resident of an in-scope country). This represents less than 50 relationships related to in-scope countries.

Whilst this still constitutes an immaterial proportion of total clients, exposure to states with active sanctions regimes still poses some risk. As of 2023, only one client was involved in activities related to dual-use items.

Lastly, there are some distribution risks associated with the onboarding and client contact model of wealth managers in Luxembourg. Furthermore, a significant amount of customer due diligence ("CDD") was performed by a third-party introducer or by a third party in the context of outsourcing or of an agency relationship. Whilst screening is still conducted by the supervised professional, given that use of intermediaries and remote engagement structures are both risk factors for sanctions avoidance, this presents some moderate risk.

5.3. Money value transfer services

Sector	Inherent risk	Sub-sectors	Inherent risk
Money Value Transfer Services	**Medium**	Payment institutions (PIs)	**Medium**
		E-money institutions (EMIs)	**Medium**
		Agents and e-money distributors acting on	**Medium**

[287] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission report: final report of the National Commission on Terrorist Attacks upon the United States*, 2004 (link)

[288] Usama bin Laden died in 2011 but remained on the UN sanctions list until February 2013 (link).

[289] Private portfolio managers carry out asset management activities (including providing investment services and custody of financial instruments) as well as some limited ancillary services (wealth structuring).

		behalf of PIs/EMIs established in another EU Member State	

Globally, MVTS providers enable cross-border transactions in a fast and convenient manner and in some cases might offer to their users products or services that may inherently favour a certain level of anonymity. This increases the sector's inherent risk of non-implementation, breach or evasion of TFS. In particular, unregulated and informal money transfer services, including hawala and other similar services providers (HOSSPs), have been and continue to be known to be abused by international terrorist groups, including ISIL, increasing the risk of exposure to persons or entities subject to TFS[290].

In Luxembourg, the vulnerability of the MVTS sector to sanctions evasion is moderate, driven by its products/services (notably the volume of transactions processed), clients and distribution model. However, there is no evidence of HOSSPs operating in Luxembourg[291]. It is also noted that HOSSPs are more prevalent in countries with a lack of banking access and low confidence in the banking system, which is not the case of Luxembourg.

In terms of size and structure, the sub-sector represented by payment institutions (PI) and electronic money institutions (EMI) is large, with 4 billion inflow transactions and 1.07 billion outflow transactions processed by 29 entities in 2023. This represents an increase since 2019 mainly due to the entry of new actors on the market as well as the increase and development of the activities of the other PI/EMI. No entity had a BO or parent from an in-scope country for PF or TF. As regards agents and e-money distributors of PI or EMI established in other European Member States (agents/e-money distributors), a small two-digit number of agents were active in 2023 in Luxembourg, compared to several thousands in the EU.

In Luxembourg, it is common for MVTS entities to offer e-money and several payment services: where some of these services are considered higher risk in international guidance (such as money remittance from a TF risk point of view). In addition, as of 31 December 2023, two PIs and one EMI are also registered as VASPs, which are flagged in FATF guidance and UN Panel of Experts' reports as having a higher risk of being exploited for the purposes of TF and PF *(for additional detail, see the cross-sector vulnerabilities section on virtual assets in section 5.11.1).* That said, not all activities conducted by MVTS entities are high risk: for example, account information services (e.g. consolidation of data) are low risk as funds are not transiting through such actors.

Payment and e-money services, by their very nature, are highly international and present inherent exposure (both directly and indirectly) to sanctioned individuals and entities. The majority of transactions facilitated through Luxembourgish PIs and EMIs are intra-EU transactions, which limits the risk. During 2023, the inflows and outflows to and from non-EU countries represented 29.72% of the consolidated flows. This included some flows reported to in-scope countries for TF in 2023, with 0.0000124% of these being reported as inflows to an in-scope country for PF. In 2022, agents/e-money distributors reported a few inflows and outflows related to in-scope countries for TF (1.1% of the total flows processed by agents/e-money distributors but 0.0005% of the total outflows processed by the whole MVTS sector). Whilst this does reduce the inherent risk exposure to some extent, it should still be noted that sanctions avoidance activities may involve circuitous flows involving several countries[292], including neighbouring countries of sanctioned states. As a result, the inherent risk is not fully alleviated by limited direct exposure.

There is inherent risk from client numbers, which are high and grew significantly since 2020 mainly due to the entry of new actors in the market and the development of the activities of the licensed entities, as mentioned above. However, very few clients/BOs are residents of in-scope countries. Moreover, among all

[290] House Homeland Security Committee, *Dismantling ISIS Financial Infrastructure*, 2016
[291] Luxembourg, *Terrorist Financing Vertical Risk Assessment* (*"*Residual risk"), 2022 (link)
[292] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, 2021 (link)

PIs/EMIs, most of the entities questioned confirmed that they exclude certain higher-risk sectors including arms, jewellery and precious metals. However, it cannot be excluded that higher risk clients are being served by certain MVTS providers[293].

Lastly, the distribution model also presents a risk of breach, non-implementation or evasion of sanctions. PIs and EMIs provide services on an online basis, which constitutes a higher risk situation according to international guidance. Meanwhile, globally agents/e-money distributors are typically considered to have less information on their clients than other more established financial institutions. This is because agents are generally less sophisticated in their compliance processes (given that agents may be small organisations such as grocery stores, conveniences stores, etc.) and have shorter-term, more infrequent relationships. That said, agents in Luxembourg all meet clients face-to-face and facilitate transactions physically.

5.4. Virtual assets service providers

Sector	Inherent risk	Sub-sectors	Inherent risk
VASPs	**Medium**	Virtual assets service providers	**Medium**

Globally, the VA and VASP space has significantly grown over the past five years. VASPs are considered as being inherently exposed to illicit financial flows and risks of non-implementation, breach or evasion of sanctions due to the pseudo-anonymity of the transactions they allow and to their decentralised nature. Indeed, the unique technological properties of VAs enable pseudo-anonymity/anonymity and fast cross-border value transfers, the execution of transactions being close to immediate and irreversible. The EU SNRA dated 27 October 2022 confirmed the higher risk exposure of VA and VASPs.

Given its role as a global financial centre and its commitment to support innovative businesses that would include VA-related activity, VASPs are present in Luxembourg. The vulnerability of the VASP sector to TF and PF TFS is overall medium, mainly driven by the products and services offered, the volume, and the immediate and irreversible nature of the transactions processed.

In terms of size and structure, the sector is very limited with only eleven entities registered as VASPs as of the end of December 2023. Out of these entities, (i) four are established outside of Luxembourg and (ii) two are authorized to operate as banks, two as payment institutions and one as an electronic money institution (all being subject to prudential supervision and representing 46% of the actors). As of the end of 2023, four entities had no activities and the sector was highly concentrated with one prevailing entity. Last, none of the VASPs had a BO or parent from an in-scope country.

As regards the products and services, as assessed in Luxembourg's ML/TF Vertical Risk Assessment: Virtual Asset Service Providers, most of the services carry a high exposure to the risk of being abused directly or indirectly by sanctioned individuals or entities. In particular, the service for exchanging VA against fiat currencies has a higher exposure as it serves as a bridge between the VA ecosystem and the "traditional" financial ecosystem. The service of safekeeping of virtual assets is also highly exposed to the risk of theft of VAs. In recent years, the illicit use of VAs was identified to be linked to cyberattacks perpetrated by both DPKR and Iran. Last, the service of transfers of VA is also highly exposed given that VA might be transferred to hosted or self-hosted wallets belonging to sanctioned naturals persons and entities.

[293] However, only one EMI confirmed having relationships with entities active in dual-use goods and export-related businesses (AML/CFT questionnaire 2022).

In Luxembourg, while there is no information regarding such abuse, the risk exists in view of the high volume of the activity. As of the end of 2023, 19.7 million transactions in VAs were exchanged and 1.3 million transfers in VAs had been executed, with a high concentration on one entity as indicated above.

In terms of clients of Luxembourg VASPs, it shall be stressed that the vast majority (99%) are natural persons. The small part of clients which are legal persons or legal arrangements are institutional clients. None of the clients nor any of their BOs are linked to DPKR or Iran. Last, none of the clients have an activity related to dual-use items or an activity with a higher risk for the raising of funds (NPOs or crowdfunding platforms).

In terms of geographies, there is no direct exposure of Luxembourg VASP activity to DPKR or Iran (no deposits of VA from and no transfers of VA to these countries). As of the end of 2023, 99% of the clients resided in EEA, UK and Switzerland. Similarly, a part of the deposits of VA comes from EEA, USA and Switzerland and the same applies for the transfers of VA. The direct exposure to countries assessed to have a higher ML/TF risk by the European Union is very limited.

Last, as regards the distribution channel, the inherent risk is by nature very high as the relationship with clients is primarily established online, on a non-face-to-face basis.

That said, it is important to note that there is no evidence that events of non-implementation, breach or circumvention of sanctions have occurred in the VASP sector.

5.5. Specialised PFSs providing corporate services

Sector	Inherent risk	Sub-sectors	Inherent risk
Specialised PFSs	Medium	Specialised PFSs providing corporate services	**Medium**
		Professional depositories	

The primary driver of TFS-related risk for Specialised PFSs providing corporate services, which are deemed high-risk in international guidance, is that corporate services can be misused to obfuscate links between transactions and designated persons/entities[294].

In Luxembourg, the Specialised PFSs providing corporate services sub-sector has an overall medium inherent risk of sanctions breach, non-implementation or evasion driven by the sector's large size and client types. Out of a total of 100 Specialised PFSs supervised by the CSSF in 2023, 85 performed TCSP activities. Taken together, they employed 7,258 workers as of 31 December 2023[295]. Of those performing TCSP activities, the top 5 entities by revenue held a 40% market share. The fragmented nature of the market, with a large number of smaller players, increases the inherent risk.

In terms of ownership model, as of 31 December 2023, no Specialised PFS had a foreign BO or parent company from an in-scope country.

The sector also has a relative degree of complexity as Specialised PFSs in Luxembourg can include various licenses, each offering different services[296]. Certain TCSP services (i.e. domiciliation, incorporation and directorship) can only be performed if the PFS has a license as corporate domiciliation agent or professional providing company incorporation and management services.

Specialised PFS can in principle provide TCSP activities, considered higher inherent risk, to any economic sector or client. The proportion of revenue derived from in-scope countries for TFS risks however is close to

[294] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, 2021 (link)

[295] CSSF Newsletter 279 (page 23), 2024 (link)

[296] Luxembourg, *National Risk Assessment* (page 97), 2020 (link)

zero, according to the last annual AML/CFT questionnaires in the sector. In terms of direct client relationships as of 31 December 2023, despite a growing number of clients, only a handful of Specialised PFS reported having in total a very small number of clients dealing in dual-use goods. These factors balance the inherent risk drivers referred above, though it should be noted that this relates only to direct client exposure (i.e. the potential for inadvertent and indirect exposure to in-scope countries via front and shell companies remains).

There are also some moderate distribution risks associated with Specialised PFSs. Over recent years, contact with some new clients was established through remote communication channels (telephone, email, online, video conference) which increases the potential risk for ultimate BOs to be hidden. Some Specialised PFSs use third parties to enter in contact with potential clients, although KYC is still rarely outsourced other than for Specialised PFSs that are part of larger banking groups as parent companies (in which case KYC may be done centrally by those banking groups and regulated under their home jurisdictions, and the CSSF requires KYC to be in any case reviewed and accepted locally by Luxembourg-based PFSs).

5.6. Insurance

Sector	Inherent risk	Sub-sectors	Inherent risk
Insurance	Medium	Life insurers	
		Non-life insurers	**Medium**
		Reinsurance	**Medium**
		Intermediaries	
		PSA	
		CAA-supervised pension funds	

As a preliminary remark, it is worth pointing out that, except where indicated otherwise, the data and statistics provided under the present section and under section 6.4.2. refer to 2023.

5.6.1. Non-life insurance

Globally, the non-life insurance sector is assessed as high-risk to the risk of breach, non-implementation or evasion of TFS related to PF and TF, primarily due to its provision of products for the maritime industry. Ships could be used by proliferators to transport restricted items or engage in banned trading activities[297], and firms could be indirectly culpable if they were found to be insuring or reinsuring vessels that are later designated as complicit in sanctioned activities[298].

In Luxembourg, this risk is assessed as moderate. Exposure to the maritime industry is existent, even if it represents only 6% of total turnover/premiums, both in 2022 and 2023. However, the sector is large and growing and, with business conducted via intermediaries and across geographies, some exposure cannot be excluded.

In terms of structure and size, the insurance sector in 2023 consisted of 263 life insurance, non-life insurance and reinsurance undertakings employing 14,493 individuals[299]. Of these, non-life insurance accounted for 38 undertakings. The 2023 premiums of the non-life sector were €19.2 billion compared to €17.52 billion at the end of 2022, up by 9.56%. The total balance sheet was €59.86 billion and the technical provisions amounted to €40.35 billion at the end of 2023. The number of employees in 2023 amounted to 9,511 across 38

[297] UK, *Proliferation Financing National Risk Assessment* (page 23), 2021 (link)

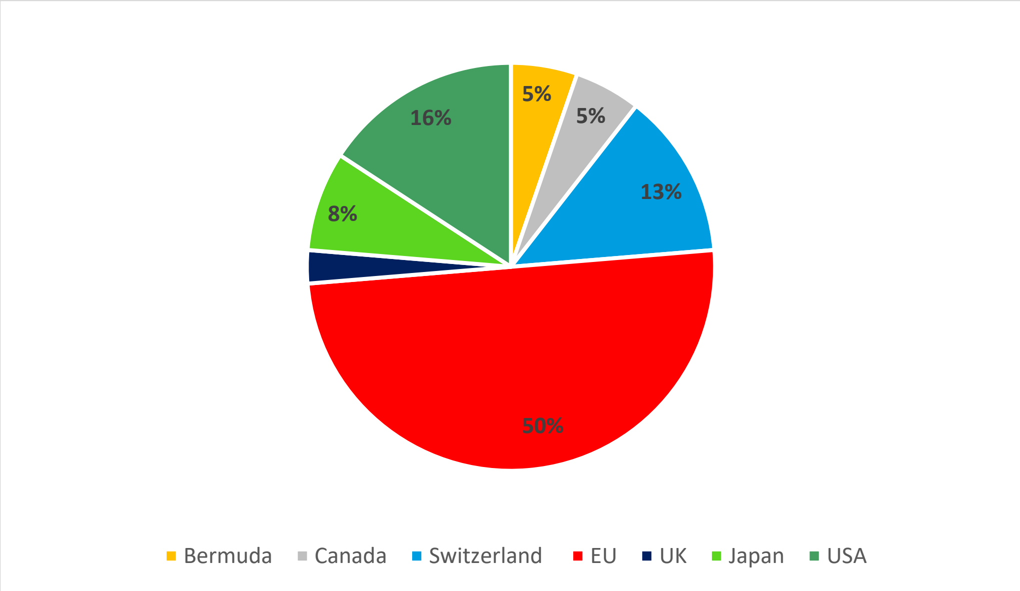
[298] Ministry of the Economy and Foreign Trade, *Luxembourg, an alternative location for shipping business*

[299] CAA annual report 2023-2024 (page 38) (link)

undertakings. The sector has grown significantly between 2019 and 2021 driven by relocations from the UK to Luxembourg due to Brexit[300]. The sector is moderately fragmented: the top 5 undertakings have a market share of around 65% in terms of gross written premium.

There is limited risk from firms' ownership structures: as at December 2023, no entities had an ultimate beneficial owner in an in-scope country. Outside the EU, the parent companies are located in Bermuda, Canada, Switzerland, UK, Japan or the USA. The chart hereunder represents the domicile of the parent company of the non-life direct insurers (excluding the special case of mutual insurance associations):

Figure 4: Non-life insurers in Luxembourg by domicile of parent company, 2023



One firm type which presents particular risk in terms of maritime exposure is P&I clubs. Luxembourg is home to three major P&I clubs conducting significant business. The third club started activity in 2021 as a consequence of Brexit. P&I clubs are mutual insurance associations providing membership to shipowners, charterers and operators with liability insurance and related services. The International Group of P&I Clubs is made of 13 independent clubs, of which two have long been established in Luxembourg (respectively since 1970 and 1977). P&I clubs have no beneficial ownership, members – who are then the policyholders of the company – having voting rights at the Annual General Meeting. The policyholders of these insurance maritime associations are shipowners who have to be members of the association before receiving an insurance coverage. That said, appropriate due diligence and sanction checks are done on each potential new member before it is accepted to the club, and the pooling of risks in the club is believed to force members to uphold each other's standards.

As at December 2023, none of the persons in charge of a key regulatory function in insurance undertakings (subject to "fit and proper" procedures) had a nationality of an in-scope country for TFS risk. Information on employee nationality and residence is not systemically collected, but it is assumed most employees of said undertakings reside either in Luxembourg (where headquarters are located) or in the country of establishment of one of their branches. The vast majorities of the branches of Luxembourg-headquartered insurance undertakings are located in an EU country, in the UK or in Switzerland, with one in Australia and very few in Asia (located in Japan, Singapore, Hong Kong and Malaysia). There are no branches located in one of the in-scope countries or in a neighbouring country.

[300] Luxembourg, *National Risk Assessment* (page 167), 2020 (link)

In terms of product mix, non-life direct insurers in Luxembourg tend to have well-diversified risk profiles. Exceptions are the captive direct insurers, one legal expense player and two health insurers, as well as the P&I clubs, which tend to be more specialised. Still, on aggregate the marine lines, deemed as a higher risk sector, represent a €1,140.5 million turnover, which represents 6% of the total turnover of €19.2 billion. The marine business in Luxembourg is very much concentrated on a small number of players: only 10 undertakings have gross written premium in excess of €3 million.

About two thirds of this business is underwritten by the three P&I clubs, the rest being provided by traditional large insurers to give a comprehensive product suite. According to a survey sent in 2021 to the insurers active in the maritime sector, the vast majority of the tonnage insured by the insurance undertakings established in Luxembourg was in Europe (50%), Asia (24%) or the Americas (8%). Very limited tonnage concerned Africa (2%) or the Middle East (4%).

According to the risk exposure of the supervised entities, there are various exclusions defined by the underwriting policy of each operator linked to type of vessels, maritime flags or transported goods (e.g. excluding certain countries, size of vessel etc.).

Table 9: Premium across top three and other selected insurance lines (€ thousands), 2020-2023

	2020	2021	2022	2023
General liability	3,454,421	4,081,834	4,398,369	4,452,335
Fire and natural forces	2,218,871	2,675,827	3,077,970	3,651,508
Inward reinsurance[301]	1,842,204	1,950,637	2,474,318	2,996,394
Goods in transit	434,972	463,815	528,447	543,635
Maritime liability	414,035	667,609	788,011	803,994
Maritime insurance	225,190	235,746	307,060	336,557

In terms of geographic spread, risk is moderate. The CAA collects data per risk location (i.e. the premium and the claims paid per risk location)[302]. The table below shows the premium collected in 2023 in countries outside of the EEA. During its desk-based review, the CAA asks for the top 5 countries in "the other countries outside EEA" category (see table below), as well as for details on premium written in countries from the FATF's black and grey lists. A significant portion of the premium written outside of the EEA is underwritten in Singapore, Hong Kong and Australia where entities have branches. Other countries are China, India, Malaysia, Panama, Saudi Arabia, Taiwan and the United Arab Emirates. There is no indication of premium underwritten in the PF in-scope countries, whilst the level of premium underwritten in the TF in-scope countries is immaterial. With regard to claims payments, the CAA has data on claims paid by line of business made to countries outside of the EEA but with no further split on these third countries. Out of total claims payments in 2023, 29% were made in relation to risks located in third countries (including the UK).

[301] Direct insurers are permitted to write a certain amount of reinsurance business in the same lines of business as they are authorized for non-life business. They are still classified as non-life insurers and must apply the same rules as for other business activity.

[302] The location of a risk is defined according to Art. 43 paragraph 17 of the modified law of 7 December 2015 on the insurance sector.

Table 10: Non-EEA premium across top three and other selected insurance lines (€ thousands), 2023

	Japan	Switzerland	United Kingdom	United States of America	Other outside EEA	Total
General liability	6,104	157,605	319,149	147,277	385,096	1,015,231
Fire and natural forces	65,780	77,772	154,448	126,580	255,442	680,022
Inward reinsurance[303]	39,545	82,851	304,879	132,899	819,581	1,379,755
Goods in transit	294	19,125	15,962	36,830	17,608	54,604
Maritime liability	32,009	2,057	12,111	45,019	537,184	628,380
Maritime insurance	745	3,872	31,749	22,765	36,287	95,417

Finally, there are some risks related to the distribution model of non-life insurers. Firstly, the use of intermediaries poses some risk. The majority of the underwriting goes through brokers (73% for new premiums underwritten in 2023 for new contracts, excluding automatic renewals) and agents and insurance agencies (11%), which need to be registered entities with EU member state competent authorities[304]. Other forms of distribution include banks and other financial institutions (5%) and direct sales (5%). In terms of payment models, premiums cannot be paid in cash and virtual assets are not currently used in the sector.

5.6.2. Reinsurance

Globally, sanctions-evasion risk in the reinsurance sector can be driven by the removal of the reinsurer from the original underwriting process. Moreover, there is potential risk derived from links to ships which could be owned, controlled or operated, including through illicit means, by a sanctioned entity[305]. International guidance also points towards reinsurance schemes as possible to be abused by perpetrators to obtain funds. In Luxembourg, the sector is assessed as having moderate risk exposure, driven mostly by its product offering, with moderate risks across its size, ownership model, geography and clients.

The sector can be divided into traditional reinsurance undertakings and reinsurance captives. Traditional reinsurance undertakings provide insurance for other insurance undertakings wanting to limit their exposure in the event of large property damages and casualty losses. Reinsurance captives are defined by the International Association of Insurance Supervisors (IAIS) as entities directly or indirectly created and owned by industrial, commercial or financial entities (the “ceding companies”), the purpose of which is to provide reinsurance cover for risks for the entity or entities it belongs to[306].

[303] Direct insurers are permitted to write a certain amount of reinsurance business in the same lines of business as they are authorized for non-life business. They are still classified as non-life insurers and must apply the same rules as for other business activity.

[304] Article 286, paragraph 4, of the modified law of 7 December 2015 on the insurance sector foresees that where insurance or reinsurance undertakings use the services of an intermediary (brokers or agents) to market their insurance products within the EEA, they may only use the services of intermediaries registered under Directive (EU) 2016/97 on insurance distribution, either by the CAA or by a competent authority of another Member State.

[305] FATF, *Guidance on Counter Proliferation Financing*, 2018 (link)

[306] See also Luxembourg, *National Risk Assessment* (page 104), 2020 (link)

The sector is relatively large (although still smaller than the life insurance sector), which increases risk exposure. The 2023 premiums reached €14.26 billion compared to €13 billion at the end of 2022. This represented a premium growth of 9.63% in 2023 compared to the previous year. At year-end 2023, the number of entities amounted to 195 with a total balance sheet of €54.88 billion. Large traditional reinsurers, which make up around 68% of the total premium volume, are typically traditional big players focused on property, casualty, and general liability. Out of the total premium written in 2023, around 17% was written by captive companies. These represent 144 companies out of the total (195) registered in Luxembourg.

There is limited risk posed by reinsurance firms' ownership models. As at 2023, none of the persons in charge of a key regulatory function in reinsurance undertakings (subject to "fit and proper" procedures) had a nationality of an in-scope country for TFS risk. Information on employee nationality and residence is not systemically collected, but it is assumed most employees of said undertakings reside either in Luxembourg (where headquarters are located) or in the country of establishment of one of their branches. There are no branches located in one of the in-scope countries or in a neighboring country. All branches of reinsurance undertakings are located in the EU, except for one branch located in Switzerland. In terms of ownership structures, as at December 2023, 91% of the reinsurance entities had an ultimate beneficial owner based in the EU. No entities had a foreign ultimate beneficial owner in an in-scope country. Outside the EU, the parent companies are located in Bermuda, Brazil, Canada, Switzerland, Japan, China, Algeria, Mexico, Panama, the UK and the USA.

In the case of captive reinsurers, beneficial owners (in the sense of the initial policyholder of the direct insurance contract) are a company of the group the captive belongs to. The CAA has defined criteria that the ceding companies have to comply with, including that ceding companies must be located in jurisdictions with a regulatory regime close to the EU standards. As at December 2023, none of the captives established in Luxembourg belonged to a group from one of the in-scope countries or reinsured risks from an ASBL, reducing captives' risk exposure.

In 2023, most of the sector's premium was written through ceding companies located in Luxembourg (4%), Germany (14%), France (12%), other EEA countries (23%), UK (27%), Switzerland (3%), and USA/Canada (3%). Out of the 14% remaining, the vast majority of the risks were underwritten in Bermuda, Brazil, India, Gibraltar, Guernsey, Japan, Singapore, Taiwan and Hong Kong. There is no premium underwritten in the PF in-scope countries, whilst the level of premium underwritten in the TF in-scope countries is immaterial.

Counterparties in reinsurance contracts are typically a direct insurance or reinsurance undertaking (hence subject to insurance regulation and supervision). Clients from large traditional reinsurers are mainly EU-based insurers or reinsurers.

The primary product risk is driven by association with the maritime sector, although this is relatively small in Luxembourg. Large traditional reinsurers, which make out around 68% of the total premium volume, offer all business classes and have a diversified profile in terms of risks accepted. Captive reinsurers cover the risks of their group and hence offer only the products needed for that objective. The CAA has information on the premium written by type of reinsurance product and the volume of premium written for maritime, aviation and transport insurance combined amounts to €849.6 million, hence 6% only of the total volume of reinsurance premiums written. Whilst maritime-only business cannot be disaggregated from this total, it is assumed to be small as the maritime business does not concern captive reinsurers.

There is some risk linked to reinsurers' distribution model, although this is limited. For captive insurers, there is direct oversight of the original insurance contract. For "traditional" reinsurance, the ceding company is expected to provide detail on its underlying portfolio, with the reinsurer using a risk-based approach to decide how and when to take on such risk.

5.7. Legal professions, chartered accountants, statutory auditors, and accountants

Sector	Inherent risk	Sub-sectors	Inherent risk
Legal professions, chartered accountants, statutory auditors, and accountants	High	Lawyers	**Medium**
		Notaries	**High**
		Bailiffs	
		(Approved) statutory auditors and (approved) audit firms (*réviseurs d'entreprises (agréés)* and *cabinets de révision (agréés)*)	**Medium**
		Chartered professional accountants (*experts-comptables*)	**High**
		Accountants	**High**
		TCSPs – professional directors	**High**
		TCSPs – business centers	**High**

5.7.1. Lawyers

Globally, lawyers play an important role as gatekeepers and intermediaries for financial transactions[307] and this makes them inherently exposed to sanctions-related risks. They possess relevant legal expertise, offer a variety of different services to their clients and typically have favourable external credibility due to their professional status. However, one should recall that terrorist financers seek to maximise the gathering of funds and would likely not spend too much legal fees. The higher risk services provided by lawyers globally relate to when they are involved with TCSP activities in addition to their core activities[308]. However, it should be noted from the 2021 and 2022 general and sub-sectoral off-site questionnaires that less than 5% of the OAL members do provide TCSP activities.

In Luxembourg, lawyers have some exposure to risks of sanctions breach, non-implementation or evasion, driven by the sector's size and product suite. As of October 14, 2022, there were 3,490 lawyers working across 578 law firms[309], all being supervised either by OAL or by OAD. OAL supervises 3,437 professionals operating in 547 different law firms organised as partnerships or legal persons, with approximately 35% of lawyers employed by the nine largest law firms (more than 50 lawyers) and a long tail of small firms (493 law firms with less than 10 lawyers, 236 with one lawyer). OAD supervises the remaining 53 professionals operating in 31 different law firms. Most law firms are owned or controlled by Luxembourg beneficial owners.

The services offered by Luxembourg lawyers are broad and this also exposes them to inherent risk, although TCSP activities are relatively limited, as shown above. Besides the traditional activities such as assistance and representation of clients in litigation proceedings (which remains the most common activity led by the OAL members), the services may include higher-risk activities including TCSP activities (to a very limited extent though). Services may also include legal advice for a variety of activities in financial and non-financial sectors, assistance or representation of clients in financial and real estate transactions and provision of advice in relation to corporate structures and other legal arrangements for clients. Generally speaking,

[307] Luxembourg, *National Risk Assessment* (page 112), 2020 (link)
[308] Luxembourg, *National Risk Assessment* (page 113), 2020 (link)
[309] Includes incorporated firms and partnerships.

large and medium-size law firms tend to practice activities relating to business law (investment funds, banking and financial law, etc.), while small law firms, associations and lawyers practicing on an individual basis mainly practice activities relating to litigation. Meanwhile, OAD lawyers' activities are mostly oriented towards litigation[310]. As of 15 September 2022, only 5% of the 3,230 OAL members (natural persons) offered TCSP services, which represented less than 1% of the sector's total turnover. As of 31 December 2023, only 101 OAL members provided TCSP services (a 38.5% decrease compared to the previous year), including only 83 providing domiciliation services (2.4% of OAL members): domiciliation activity (which represented approximately 60% of the TCSP activities performed by OAL members) decreased by approximately 17% in one year. This decrease is the result of both an ever-increasing awareness of the risks associated with TSCP activities and a reduced risk appetite for this kind of activities. Other TCSP activities are very marginal, as only 2 OAL members perform a fiduciary activity and only 3 OAL members perform a trustee activity. In addition, it can be noted that the number of OAL members acting as depository of bearer shares decreased from 27 to 20.

The profession's large and international client base is also a driver of inherent risk. Luxembourgish lawyers serve a wide range of clients and international business, with a wide diversity of non-resident clients and transactions[311]. Moreover, clients' nationality/country of residence can present some moderate risk. In this respect, based on the data collected from the OAL's November 2021 off-site questionnaire, 93 lawyers/50 law firms (3% of the lawyers and less than 10% of the law firms) had indicated having clients who were either nationals or resident of some in-scope jurisdictions. These lawyers/law firms have been subsequently contacted (via a sub-sectorial off-site inspection), on an individual basis, by the Commission de Contrôle du Barreau de Luxembourg ("CCBL")[312] to ascertain the type of services performed for these clients. It appears that none of the services performed were in relation with financial transactions or TCSP activities. Indeed, all of these services were rendered in connection with either (i) assistance relating to application of refugee status or (ii) legal aid.

Besides the in-scope countries, 1.36% of the lawyers/law firms have indicated having clients or beneficial owners who are either resident or nationals of other high-risk jurisdictions. In this case, the lawyers/law firms declare that their internal policies address the higher risk arising therefrom. Moreover, only 2.5% of the lawyers/law firms questioned declared having PEPs among their clients. Looking at clients from higher risk sectors, less than 2% of the lawyers/law firms declared having clients who conduct activities in relation to virtual assets, maritime transport, dual-use goods or are NPOs.[313]

The distribution model of lawyers also drives some inherent risk, as clients are sometimes acquired via intermediaries and non-face-to-face interaction can occur[314]. This could decrease lawyers' visibility of potential sanctions-avoidance activity. That said, from January to November 2021, clients were acquired via direct contact in 88% of cases. For the remaining 12% acquired via intermediaries, 10% related to intermediaries being themselves professionals subject to the 2004 AML/CFT Law. It is also worth mentioning that KYC and ongoing monitoring must still be conducted by the law firm, and reliance on intermediaries only concerns the collection of documentation.

[310] Luxembourg, *National Risk Assessment* (page 114), 2020 (link)
[311] Luxembourg, *National Risk Assessment* (page 114), 2020 (link)
[312] The CCBL is in charge of carrying out (upon delegation of the Bar Council) every inspection (on and off-site) in lawyers' offices (art. 8-2bis of the 2004 AML/CFT Law).
[313] Off-site questionnaire conducted by OAL, November 2021.
[314] Luxembourg, *National Risk Assessment* (page 114), 2020 (link)

5.7.2. Chartered professional accountants (*experts-comptables*)

Globally, chartered professional accountants (CPAs) provide a key gatekeeper and intermediary role for transactions, which makes them inherently exposed to sanctions-related risk. Many also conduct TCSP activities, which present some risk exposure as shown by their status as a higher-risk activity in FATF guidance[315].

In Luxembourg, CPAs have a high risk of sanctions evasion, primarily driven by the sector's size, fragmentation and client types. The sector is large and fragmented, with approximately 1,232 CPAs spread across approximately 560 legal entities and 66 independent professionals[316]. The OEC is responsible for overseeing sole practitioners and legal entities of varying sizes. Significantly, more than 75% of these entities have fewer than 10 employees, while 53% report annual revenues below €500,000. Furthermore, fewer than 2% of registered legal entities employ more than 250 individuals.

Table 11: Breakdown of TCSP services offered by OEC member firms, 2023[317]

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	0.71%	0%	0%	0%	100%

Given the relatively low number of sole practitioners offering TCSP services, the table 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 with a broader oversight of their clients' activities.

[315] FATF, *Guidance of Proliferation Financing Risk Assessment and Mitigation* (page 24), 2021 (link)

[316] The exact figures vary on a monthly basis.

[317] Data collected through the 2024 RBA questionnaire (pertaining to 2023 data). Note that TCSP activities remain relatively consistent year after year.

The CPA profession's large and international client base is also a driver of inherent risk. At the end of 2023, there were a total of 111,164 clients, including 811 offshore companies, 152 foundations and 687 non-profit organisations. Furthermore, 60.8% of respondents reported having beneficial owners who were non-EU nationals in their client base.

5.7.3. (Approved) statutory auditors and (approved) audit firms (*réviseurs d'entreprises (agréés)* and *cabinets de révision (agréés)*)

Globally, statutory auditors may present some risk of sanctions evasion, as they can carry out TCSP activities which present a higher-risk activity in FATF guidance[318].

In Luxembourg, the audit profession is assessed as having a medium risk of sanctions evasion, driven primarily by the sector's size and distribution, as well as some limited exposure to TCSP activities. The audit sub-sector in Luxembourg is a sizeable and moderately fragmented profession, with 66 audit firms[319] and 636 statutory auditors[320,321,322,323]. Statutory auditors are predominantly nationals of EU Member States[324] and none are nationals of countries subject to the PF or TF sanctions regimes in scope of this report. In addition, based on responses to the annual Risk Based Approach questionnaire[325] ("RBA questionnaire"), no Luxembourg-based audit firms have any branches or subsidiaries in in-scope countries[326], reducing risk of breach, non-implementation or evasion of sanctions related to PF and TF.

The core activities for the audit profession include auditing financial statements and are believed to be lower-risk for PF and TF sanctions risk purposes. That said, statutory auditors may perform TCSP activities. This presents some risk exposure given their status as a higher-risk activity in FATF guidance[327].

[318] FATF, *Guidance of Proliferation Financing Risk Assessment and Mitigation* (page 24), 2021 (link)

[319] In this document, the term "audit firm(s)" covers equally "audit firm(s) and "approved audit firm(s)" unless the precision is required.

[320] In this document, the term "statutory auditor(s)" covers equally "statutory auditor(s) and "approved statutory auditor(s)" unless the precision is required.

[321] Based on the CSSF's register as at December 22, 2023.

[322] For the definition of statutory auditors, approved statutory auditors, audit firms and approved audit firms, reference should be made to the Law of 23 July 2016 on the audit profession.

[323] As of 22 December 2023, 77% of (approved) statutory auditors are active in public practice and 23% are active in business. 62% of (approved) statutory auditors are spread across seven approved audit firms.

[324] As of 3 March 2022, 92.9% from EU member states and 84.7% from Luxembourg and neighboring countries (Belgium, France and Germany).

[325] Based on 2023 RBA questionnaires provided in February and March 2024.

[326] This excludes international networks of Luxembourg-based firms, which may have firms in in-scope countries.

[327] FATF, *Guidance of Proliferation Financing Risk Assessment and Mitigation* (page 24), 2021 (link)

Statutory auditors are subject to some limited international exposure, with no client registered in an in-scope country[328].

Statutory auditors serve a wide variety of clients both from the financial and the non-financial sectors, in Luxembourg and internationally, due to the nature and size of Luxembourg's financial centre and its diverse population. Despite this, there are very few business relationships reported with nationals or PEPs of in-scope countries. Statistics for the whole audit profession show that only 5[329] beneficial owners of audit firms' clients are resident in an in-scope country. No clients of an audit firm had in 2023 a beneficial owner which was a PEP resident in an in-scope country and one person purporting to act on behalf of or for one audit firm's client was resident in an in-scope country in 2023. In addition, 0.29% of the total clients of the audit profession in 2023 were NPOs operating abroad[330].

The distribution model of statutory auditors presents some moderate risk. The IRE controls compliance with law requirements when such circumstances exist.

5.7.4. Notaries

Globally, whilst the exact role of the notarial profession varies according to a jurisdiction's legal regime[331], the types of activities they support present an inherent risk of facilitating TFS non-implementation, evasion or breach. In particular, the FATF notes notaries' role in the formation of companies and trusts as a key risk factor, given that front and shell companies may be used to obfuscate beneficial ownership[332]. Notaries are also important "gatekeepers" when setting up company structures and, to a lesser extent and under specific circumstances, provide further customised services to companies during their lifecycles. This may include submitting business information to registers and the updating of deeds, which in turn could also be exploited to evade TFS.

In Luxembourg, the inherent risk related to sanctions breach, non-implementation or evasion is assessed as high for notaries. This is primarily driven by the nature of services that notaries perform, rather than by the size of the sector or its interaction model. Indeed, in 2021 there were 36 notaries in office in Luxembourg[333], as well as approximately 250-350 professionals[334]. Among these are in-house lawyers (*juristes collaborateurs*) specialising in notarial law and other experts in notarial law, notary clerks, accountants (for the internal accounting of the respective notarial office) and/or assistants[335]. Luxembourg law now allows the appointment of non-Luxembourg nationals to the profession, but there were in 2023 no nationals or dual nationals of in-scope countries in the Luxembourg notariat[336].

As assessed in the 2020 NRA, notaries in Luxembourg act as important gatekeepers to many business acts, including legal entity set-up, credit opening, sale of business and mergers,[337] which – as in other jurisdictions – exposes them to the types of risks mentioned above. Notaries are not the direct agent responsible for company formation within the meaning of TCSP activities, but they are responsible for submitting companies' registration information, as well as any updates on a regular basis, to Luxembourg's registers (the RCS and, if requested by the client, the RBE). They have privileged access to clients' registered

[328] Based on 2023 RBA questionnaires provided in February and March 2024.

[329] Based on 2023 RBA questionnaires provided in February and March 2024.

[330] NPOs operating only within Luxembourg are not in scope of this figure.

[331] FATF, *Risk-based approach for legal professionals*, 2019 (link)

[332] FATF, *Risk-based approach for legal professionals*, 2019 (link). It should be noted that trusts cannot be formed in Luxembourg and that Luxembourg notaries do not play any role in the creation of *fiducies*.

[333] The number of notaries is capped by law at 36.

[334] Data provided by CdN for the purpose of this risk assessment.

[335] Luxembourg, *National Risk Assessment* (page 111), 2020 (link)

[336] Data provided by CdN for the purpose of this risk assessment.

[337] Luxembourg, *National Risk Assessment* (page 111), 2020 (link)

information with LBR and must also inform the RBE if they detect any mismatch between the information on the RBE and the information the client has provided them with. These activities may be exposed to the risk of misuse or abuse by designated individuals; the use of complex legal structures is well evidenced in international guidance such as FATF and UN PoE reports as a primary typology for sanctions avoidance or evasion.

In addition to the higher risk activities described above, some notaries focus their activities in the area of corporate law rather than business services, which was the predominant activity of 7 notaries in 2020. The activities of these mostly midsize respectively larger notarial offices represent a smaller portion of the overall general business of the Luxembourg notaries. The majority of notarial deeds set up in Luxembourg concern private individuals, with international companies playing a minor role and, in some notarial offices (especially those situated in non-metropolitan areas), an insignificant role. Notaries also screen clients regularly and the percentage of their individual clients who are PEPs is low. In 2020, across all notaries, 40 clients were PEPs from third countries, including, in a very limited number of cases, Gulf countries (excluding Iran and Iraq), Saudi Arabia, Russia and India.

Non-face-to-face business interactions are extremely rare with natural persons, but with legal entities can in certain cases take place via intermediaries. Some notaries reported increased use of proxies during the COVID-19 pandemic, which presents risk as it could make it easier to hide BO. Indeed, one notary reported the usage of falsified documents during 2020. In this case, the notary was asked by the third person whether a specific attestation of signature (*légalisation*) had actually been set up by the notary. The verification by the notary revealed that it was not the case and that the attestation of signature had been falsified by the third person's client.

5.7.5. Accounting professionals

Globally, accounting professionals[338] can provide TCSP services which are flagged in international guidance as having an inherent risk of sanctions evasion. Entities may also use intermediaries which limits overall transparency/visibility, thereby potentially making it easier for designated entities to obfuscate their BO when using accounting professionals.

In Luxembourg, alongside the inherent product risk, the large and international nature of the accountant sub-sector drives its overall risk of sanctions evasion. As of 31 December 2023, there were in the country 651 accounting professionals[339]; among these, the top 100 accounting professionals represented 73.6% of the market turnover while the top 5 accounting professionals represented 20% of the market turnover, suggesting a high degree of market fragmentation.

Many accountants limit themselves to providing services such as payroll, preparation of VAT returns, preparation of personal income tax returns, administrative activities, and encoding activities for a CPA[340]. Although the Law of 31 May 1999 governing the domiciliation of companies as amended (the "1999 Domiciliation Law") prohibits them from providing domiciliation services, they may, however, provide other TCSP services that are not reserved for professionals. As noted in the 2020 NRA, there is also a large component of international business involved in the activities of accounting professionals, which exposes the sub-sector to international flows. That said, based on a sample of 73 accounting professionals in 2021, only 0.53% of clients were reported as being non-EU residents. Whilst it is not possible to generalise this

[338] The term "accounting professionals" herein refers only to the professionals supervised by AED. Chartered professional accountants are supervised by OEC and so are excluded from this inherent risk assessment.

[339] Data provided by AED for this risk assessment, 2024.

[340]Data provided by AED for this risk assessment, 2021.

figure for the whole sector, it does suggest that overall exposure to nationals/dual nationals of in-scope countries is relatively low.

5.7.6. TCSPs: business centres and professional directors

Globally, TCSP activities are considered as inherently vulnerable to sanctions evasion, given their ability to obfuscate links between transactions and designated persons/entities[341]. TCSP services are varied but can include creating entities (such as shell and front companies) as well as providing domiciliation or shareholder nominee services, which could reduce the transparency of a transaction.

In Luxembourg, the inherent risk associated to TCSP business centres and professional directors is compounded by the sector's size and the diversity of services provided, which may create exposure to sanctions-evasion typologies. Nonetheless, the sector is subject to a comprehensive regulatory and supervisory framework, and the implementation of risk-based mitigating measures substantially reduces the likelihood and impact of such misuse. In 2020, there were 60 business centres operational in Luxembourg[342], which provide varied TCSP services. Business centres provide domicile services and "*services liés*" (related services) to entities, which may include a variety of activities such as reception service, telephone service, or postal mail delivery[343]. However, business centres may also register companies that do not have physical presence at the centres and as such have limited visibility on these companies' activity. In 2020, business centres reported a turnover of €46.3 million[344]. Based on a sample of 31 business centres in 2021, 3.59% of their clients were situated outside of the EU.

In 2022, there were also 201 professional directors (natural persons) registered for VAT purposes[345] with the AED[346]. Any natural or legal person can act (or arrange 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. According to research and analysis carried out by the AED from 2019, 13 professional directors account for 44% of the profession's overall turnover[347]. Professional directors may be inadvertently involved in the activities of a designated person or entity. That said, they are also liable for any actions they approve[348], and thus have the incentive to ensure an appropriate level of control is applied over the actions and transactions they are approving, which could reduce some of the risk. TCSPs such as business offices and professional directors are also often exposed to multiple jurisdictions, reflecting the attractiveness of Luxembourg as an international financial centre[349]. This increases complexity when it comes to identifying beneficial owners, thereby increasing the risk further for sanctions evasion.

Lastly, the clients that use TCSPs generally have a highly sophisticated understanding of the financial system and may use intermediaries. This increases the anonymity of the relationship, which may make it easier for designated entities to obfuscate their true activity/their relationship to the PF or TF value chain.

---

[341] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 24), 2021 (link)
[342] Data provided by AED for this risk assessment, 2021.
[343] Luxembourg, *National Risk Assessment* (page 116), 2020 (link)
[344] Data provided by AED for this risk assessment, 2021.
[345] Data provided by AED for this risk assessment, 2021.
[346] Data provided by AED for this risk assessment, 2021.
[347] Data provided by AED for this risk assessment, 2021.
[348] Luxembourg, *National Risk Assessment* (page 142), 2020 (link)
[349] Luxembourg, *National Risk Assessment* (page 141), 2020 (link)

All corporate systems have a process for obtaining basic information on corporate entities as a preliminary requirement for the formation of such entities. The purpose of this process is to identify the legal owner of the company, as well as the responsible and liable person for a given situation (including for commercial purposes or for civil/criminal liability matters). This basic information includes the company's name, proof of formation, legal form and status, registered office's address, signing powers, name (precise role) of those through whom the entity acts, basic governance rules, signatory powers (e.g. via the company's memorandum or articles of association), and a register of shareholders or members containing the number of shares held by each shareholder and categories of shares (including the nature of the associated voting rights). This information must be contained in the register and must be accurate and up to date. Moreover, the ability to obtain accurate and up-to-date basic information in a timely manner is a preliminary condition to obtaining BO information, as it is generally the legally liable person who provides the BO information of registered entities.

RCS registry

All legal persons set up under Luxembourg law must be registered with the RCS as per the Law of 19 December 2002 on the Trade and Company Register[350] (the "2002 RCS Law"). The RCS is managed by Luxembourg Business Registers (LBR), an economic interest group placed under the authority of the MoJ, which includes the Luxembourg State and the Chambre de Commerce. LBR's mission is to manage and develop the different registers under its remit. Each of these registers has its own legal framework. LBR is also in charge of the electronic central platform for official publications, namely the Electronic Compendium of Companies and Associations (RESA) since 1 June 2016, as well as the RBE, established on 1 March 2019. The 2002 RCS Law lists the information that entities must register with the RCS. One part of this information is descriptive data (basic information – e.g. name, members of board of directors, capital, etc.), while the other part is related to accounting information. This information must be accurate and up to date. Entities must update their information within the month of the event leading to a change in their data (article 15 of the 2002 RCS Law). LBR is also in charge of registering the financial statements of companies. Said registration is mandatory for some types of legal persons, whereas for others it depends on certain factors, such as amongst others reaching an annual turnover threshold.

TCSPs: AML/CFT gatekeepers

Professionals must comply with their obligations under the 2004 AML/CFT Law when offering TCSP services. This helps mitigate the vulnerabilities for legal persons and legal arrangements in the corporate risk, as TCSPs are able to obtain basic information and BO information including when there is a request from relevant authorities. In Luxembourg, different types of professionals can provide TCSP services. They must, in all cases, implement the preventive AML/CFT measures (as set out below) of the 2004 AML/CFT Law. The following table shows the different types of professionals that can provide TCSP services and their national AML/CFT competent supervisory body.

[350] Law of 19 December 2002 on the Trade and Company Register and companies and on bookkeeping and annual accounts of companies and amending certain legal dispositions (link)

Table 12: Different types of professionals falling within the definition of a TCSP and their AML/CFT supervisor/SRB[351]

AML/CFT supervisor/SRB	Professional authorized to carry out TCSP activities
CSSF	Banks and credit institutions
	Investment firms
	Management companies
	Regulated securitisation undertakings/vehicles
	Three types of specialized professionals of the financial sector, including with the following licenses: - Family offices - Corporate domiciliation agents - Professionals providing company incorporation and management services
CAA	Professionals of the insurance sector
OEC	Chartered professional accountants
IRE	(Approved) statutory auditors and (approved) audit firms
OAL/OAD	Lawyers (List I and IV of the Bar)

In addition to the licensing/qualification requirements for the types of professionals supervised by the CSSF, CAA, OEC, IRE and OAL/OAD, the 2004 AML/CFT Law requires them to register as TCSP with their respective supervisory authority or SRB, unless the supervisory authority has granted an exception. TCSPs play a significant role in the prevention of ML/TF. Even before the actual creation of the legal persons or legal arrangements, they must perform CDD controls when providing support to the setup of legal persons and legal arrangements. Moreover, once the legal person or legal arrangement has been created, these professionals maintain a long-term business relationship with their corporate clients, allowing the professionals not only to update and keep accurate CDD information but also to acquire an overall good knowledge of their clients, their activities, as well as their directors, managers, shareholders and BOs. This is particularly true when a single TCSP offers multiple services simultaneously to a client (for instance where the TCSP offers both domiciliation and directorship services to an entity) and it is particularly useful when monitoring the business relationship – i.e. to detect ML/TF-related suspicious behaviour. Furthermore, these TCSPs are required to scrutinise the transactions undertaken by clients based on materiality and risk to ensure that they are consistent with their knowledge of the customer, of their business and risk profile, and of their sources of funds and where applicable wealth. These activities include name screening as well as transaction monitoring. These professionals also have an obligation to file suspicious transaction reports (STR) and suspicious activity reports (SAR) to the CRF. As stated in the above table, various professions fall within the definition of a TCSP and are subject to the 2004 AML/CFT Law. With the exception of the entities that fall under the supervision of the IRE and the OEC, none of the regulated professions are supervised by two or more supervisors. For the IRE and the OEC, the respective supervisory bodies have clearly identified which professionals are simultaneously controlled by both. Furthermore, with the adoption of the Law of 25 March 2020, the exchange of information between SRBs is allowed and the IRE and the OEC are coordinating their actions with regard to "common" members. In fact, as stated by article 9-1 of the 2004 AML/CFT Law, supervisory authorities and SRBs shall cooperate closely among themselves. More specifically, pursuant to article 7-2, paragraph 3, supervisory authorities and SRBs should coordinate with each other in order to set

[351] Luxembourg, *ML/TF Vertical Risk Assessment Legal Persons and Legal Arrangements*, 2022 (link)

up a list of the TCSPs for which they are competent. It should also be noted that supervisory authorities and SRBs do cooperate on a regular basis. This occurs both at the level of the National Prevention Committee (i.e. the main co-ordination mechanism for AML/CFT in Luxembourg) and informally through bilateral exchanges on specific questions, including the implementation of the risk-based approach and AML/CFT supervisory practice.

Domiciliation

One of the services that TCSPs offer is domiciliation. The 1999 Domiciliation 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 1999 Domiciliation Law requires that the domiciled company and the domiciliation agent conclude a written agreement called a domiciliation contract. As such, domiciliation services are a way of conducting business that provides third parties with a seat and other 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 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 Ministry of the Economy in accordance with the Law of 2 September 2011 regulating the access to different professions of craftsman, trader, industrialist, as well as to certain liberal professions (the "2011 Business Licenses Law"), which specifically states that a domiciliation within the meaning of the 1999 Domiciliation Law does not constitute an establishment. Operational companies established in Luxembourg therefore cannot use such domiciliation services. Pursuant to articles 100-2 and 1300-2 of the 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 the seat of 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 chartered professional accountant. The IRE and the OEC require (approved) statutory auditors and chartered professional accountants 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. Furthermore, the CSSF has 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". 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 the latter (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, 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 between €1,250 and €12,000.

5.8. Dealers in high value goods

Sector	Inherent risk	Sub-sectors	Inherent risk
Dealers in high values goods	**Medium**	Precious metals, jewelers and clocks	**Medium**
		Car dealers	**High**
		Art/antiques	**Medium**
		Luxury goods	**Medium**

Globally, the anonymity and bearer-instrument nature of high value goods such as precious stones, art or luxury items makes dealers of those goods vulnerable to sanctions evasion or breach. FATF guidance, for instance, highlights the potential use of precious metals and stones to transfer financial resources across borders[352], whilst the UK noted the potential for luxury goods to be purchased by DPRK and then resold to richer members of the North Korean population, which could indirectly fund proliferation activities[353]. Moreover, UN Monitoring Team reports have also highlighted that ISIL and Al-Qaida have exploited and monetised artisanally mined gold, particularly in conflict zones[354]. As with many other examples of sanctions evasion, shell companies and intermediaries can be used to obfuscate beneficial ownership further when dealing in high-value goods[355].

As per the national risk assessment, this sector is split into four sub-sectors: i) precious metals, jewelers and clocks, ii) luxury goods, iii) car dealers, and iv) arts & antiques dealers.

For dealers in precious metals, jewellery and clocks, there is a medium inherent risk of sanctions evasion. There were, as of 2023, 130 entities active as dealers in precious metals and stones ("DPMS"), which make up the majority of this sub-sector, and their aggregate turnover was €123 million (with the top five entities representing 55% of the total)[356]. The products – particularly gold and silver – are flagged in FATF and UN PoE reports as vulnerable to exploitation for sanctions avoidance or evasion, particularly where the value of goods is high.

Luxury goods dealers have a medium inherent risk of sanctions evasion. Whilst the sub-sector is believed to be highly concentrated in Luxembourg, the products are listed in international guidance as vulnerable to exploitation by designated individuals on sanctions lists. This is also evidenced by the fact that luxury goods are subject to export controls, particularly with reference to DPRK.

---

[352] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (page 24), 2021 (link)
[353] UK, *National Risk Assessment of Proliferation Financing* (page 20), 2021 (link)
[354] UN, *Monitoring Team's Twenty-eighth report* (page 18), 2021 (link)
[355] OFAC, *Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork,* 2020 (link)
[356] Data provided by AED for this risk assessment, 2025.

Car dealers are assessed as having a high inherent risk due to the sub-sector's products and activities as well as the sub-sector's structure (i.e. size and fragmentation), international nature of the business and types of clients/transactions (i.e. volume and risk). Luxury cars could constitute an anonymous storage of value and medium of exchange for designated individuals and entities, similar to precious stones, which drives some moderate risk. There were 650 entities in the sub-sector in 2023, reporting a global turnover of €5.1 billion.

Finally, art & antiques dealers have a medium risk of sanctions evasion. In 2020, 133 were recorded by the AED, at a total turnover of €45.6 million. Whilst they could still be leveraged for cross-border movement of goods and store of value, similarly to precious stones, they represent a relatively small sector in Luxembourg and exposure can thus be deemed moderate.

5.9. Freeport

Sector	Inherent risk	Sub-sectors	Inherent risk
Freeport	**Medium**	Freeport operators	**Medium**

Globally, the high security and confidentiality afforded to the clients of freeports presents inherent risk, as does the fact that there may not be full information on the ultimate beneficial ownership of items, driven by the use of nominees[357].

In Luxembourg, the Freeport presents a risk of sanctions evasion due to its internationality and the nature of its products and services. The Freeport is located in Luxembourg Findel airport and encompasses 22,000 m² of building structure. It is specifically designed for the storage of high value goods (such as artwork, vintage cars, gold, luxury goods and fine wines)[358], and as such could be indirectly exposed to PF/TF sanctions evasion risk since those goods have been flagged in international guidance and in PoE reports to be attractive for designated individuals and entities. Given its nature and location, the Freeport also has large international flows – with inflows and outflows of goods being largely cross-border and for an international client base – which also contributes to the risk. The fact that the Freeport houses a significant number of items which are considered to be vulnerable to proliferators[359] further presents inherent risk. In 2023, the sector in Luxembourg comprised 5 authorised operators.

However, compared to freeports in high-risk jurisdictions – where limited regulation, significant transactional activity and broad client accessibility justify a higher inherent risk rating – the Luxembourg Freeport operates at a smaller scale, under full AML/CFT and TFS regulation, and with restricted access and limited onsite commercial activity. These structural differences significantly reduce the exposure to PF and TF TFS vulnerabilities typically associated with freeports internationally. Accordingly, while certain inherent vulnerabilities remain due to the nature of stored high value items and cross border clientele, the overall inherent risk for the Luxembourg Freeport is assessed as medium.

[357] Luxembourg, *National Risk Assessment* (page 121), 2020 (link)

[358] Luxembourg, *National Risk Assessment* (page 121), 2020 (link)

[359] Statues and luxury goods (including art, precious metals, etc.) are all subject to export controls for DPRK. Source: RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment,* 2019 (link)

The table below captures items into and out of the Freeport (based on movement notifications) for selected types of goods for the 2020-2023 period.

Table 13: Extract of data showing movement notifications of different types of goods, 2020-2023[360]

Type of goods	In	Out
Silver, unwrought or in semi-manufactured form (units)	661	90
Collections of historic interest, numismatic, etc. (units)	67	64
Diamonds (units)	0	0
Original engravings, prints and lithographs (units)	47	21
Antiques more than 100 years old (units)	9	19
Original sculptures or statuary (units)	101	119
Pictures, paintings and drawings produced entirely by hand (units)	481	314

5.10. Legal persons and legal arrangements

Sector	Inherent risk	Sub-sectors	Inherent risk
Legal persons and legal arrangements	Very High	Sociétés commerciales	Very High
		Domestic “fiducies”	Very High
		Foreign trusts	Very High
		ASBLs and fondations falling under FATF NPO definition engaged in activities abroad	Very High
		Sociétés civiles	
		Other associations sans but lucratif (ASBL)	
		Other legal entities	

Globally, legal persons and legal arrangements are vulnerable to PF and TF as the use of multiple layers of legal persons and/or arrangements is often linked to orchestrating the opacity of financial flows for TF and/or PF. As proliferation support networks become increasingly complex, legitimate institutions may become inadvertent actors in a broader chain of illicit intermediaries, brokers and front companies[361]**.** For example, the UK’s PF risk assessment provides a case study of a situation in which intermediation and legal persons and legal arrangements can together present risk. A Scottish Limited Partnership (SLP) was set up by an Eastern European business operator using a professional gatekeeper in the Baltics. The SLP acted as an intermediary for defense related contracts, but its representative resident in Scotland was completely unconnected with its business operations[362].

In 2014, a report by the FATF on the risk of terrorist abuse in NPOs[363] identified five common methods of NPO misuse, including two which may enable sanctions evasion:

a. Diversion of funds, whereby “*an NPO, or an individual acting on behalf of an NPO, diverts funds to a known or suspected terrorist entity*”.

[360] Data provided by ADA for this risk assessment, 2021.
[361] US, *National Proliferation Financing Risk Assessment*, 2018 (link)
[362] UK, *National Risk Assessment of Proliferation Financing* (pages 17-18), 2021 (link)
[363] FATF, *Risk of terrorist abuse in non-profit organisations*, 2014 (link)

b. False representation, whereby "*under the guise of charitable activity, an organisation or individual raises funds and/or carries out other activities in support of terrorism*".

In Luxembourg, the legal persons and legal arrangements sector includes *sociétés commerciales*, *sociétés non-commerciales*, including *sociétés civiles* and legal persons from the non-profit sector (which may take the form of *associations sans but lucratif* (ASBLs) and *fondations),* domestic *fiducies* and foreign trusts. This risk assessment will focus on sociétés commerciales and NPOs[364] (legal persons) and domestic *fiducies* and foreign trusts (legal arrangements).

5.10.1. Legal persons

All legal persons incorporated in Luxembourg must be registered with the RCS as per the 2002 RCS Law and must record their beneficial owners in the RBE. By its very nature, this section therefore includes firms classified in other sub-sectors[365].

As of December 2023, there were 146,373 legal persons registered with the RCS, the majority taking the legal form of sociétés commerciales. The table below captures their taxonomy in Luxembourg.

Table 14: Legal entity taxonomy

Legal entity type, as registered in the RCS	Outline of key legislation
Sociétés commerciales	As per article 100-2 of the 1915 Companies Law: • SNC (société en nom collectif) • SCS (société en commandite simple) and SCSpé (société en commandite spéciale) • SA (société anonyme) and SAS (société par actions simplifiée) • SCA (société en commandite par actions) • SARL (société à responsabilité limitée) and SARL-S (société à responsabilité limitée simplifiée) • SC (société coopérative), SE (société européenne) and SCOOP (société coopérative organisée comme une SA)
Sociétés civiles	As per article 1832 of the Civil code
Associations sans but lucratif (ASBLs)	Non-profit organisations, as per the Law of 7 August 2023
Fondations	Foundations, as per the Law of 7 August 2023
Other legal persons	All other legal entities registered with RCS, including, but not limited to: • Groupements d'intérêt économique • Groupements européens d'intérêt économique • Associations agricoles • Établissements publics

[364] Meaning ASBLs and *fondations* from the non-profit sector falling under the NPO definition.

[365] Including sub-sectors under the supervision of the Luxembourg supervisory authorities. As an example, firms licensed/registered by the CSSF are subject to several preventative measures applied both at market entry and during their daily supervision for AML/CFT, financial sanctions and prudential purposes. Such measures aim at preventing criminals from entering the sub-sectors and at continuously monitoring those supervised firms for compliance with their professional obligations. While the level of TFS inherent risk of those sub-sectors is intrinsically lower than the one assessed for the sociétés commerciales, consequently the level of TFS residual risk considering such mitigating factors is still lower (reference is made to Table 1).

Connections with in-scope countries are very limited. Based on RBE data (covering all legal entity types obliged to report BO data, not just sociétés commerciales) as of 31 December 2023, 49 beneficial owners were resident in an in-scope country and appeared as BOs of 64 entities mostly operating in the financial sector. In addition, 1,140 BOs were born in in-scope countries and 185 BOs were nationals of an in-scope country (though the majority in both cases resided in Luxembourg), in both cases associated with companies with activities spread across the financial sector (approximately 40-50%) and other sectors (commerce, restaurants, etc.), which likely reflects Luxembourg's significant immigrant community.

Based on RCS data, a few directors and shareholders (irrespective of being BO) were residents or nationals in in-scope countries. For example, 25 entities had at least a shareholder resident in an in-scope country, and 67 entities had a director resident in an in-scope country. 630 entities had at least one shareholder born in an in-scope country and 2,044 entities had a director born in an in-scope country.

Legal persons in Luxembourg also have varied activities and include entities active in the financial sector, which typically presents a higher risk for sanctions evasion. Based on NACE codes[366] registered with RCS, **there is however a limited number of legal persons in Luxembourg operating in non-financial sectors which have a higher exposure to sanctions evasion, such as the maritime sector, or those related to the export of dual-use goods.** The table below captures, for selected NACE codes, the number of legal persons registered as per the taxonomy listed in the table above.

Table 15: Number of sociétés commerciales registered on RCS by entity type for selected NACE codes[367]

Legal entities									
NACE	Description	SNC	SCS	SA/SAS	SARL	SARLS	SC	SE	Other
A3	Fishing and aquaculture				3	1			
B5	Mining of coal and lignite								
B6	Extraction of crude petroleum and natural gas								
B7	Mining of metal ores								
B8	Other mining and quarrying			5	7				
B9	Mining support service activities								
C13	Manufacture of textiles			4	9				
C16	Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials			10	12				1
C19	Manufacture of coke and refined petroleum products				1				

[366] NACE is a four-digit classification system used in the EU to list economic sectors.

[367] NACE codes selected based on RUSI's guidance regarding goods subject to export control. Source: RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment* (page 10), 2019 (link); table concerns sociétés commerciales only (i.e. companies registered as ASBLs or sociétés civiles are excluded).

Legal entities									
NACE	**Description**	**SNC**	**SCS**	**SA/SAS**	**SARL**	**SARLS**	**SC**	**SE**	**Other**
C20	Manufacture of chemicals and chemical products			8	6	1	1		
C22	Manufacture of rubber and plastic products			18	8				
C23	Manufacture of other non-metallic mineral products			25	17				
C24	Manufacture of basic metals			10	3				
C25	Manufacture of fabricated metal products, except machinery and equipment			100	171	7			5
C26	Manufacture of computer, electronic and optical products			5	7				
C27	Manufacture of electrical equipment			6	5				
C28	Manufacture of machinery and equipment n.e.c.		1	13	20				
C29	Manufacture of motor vehicles, trailers and semi-trailers			3	6				
C30	Manufacture of other transport equipment				3				
C32	Other manufacturing			14	74	5			
C33	Repair and installation of machinery and equipment			23	48	1			
G45	Wholesale and retail trade and repair of motor vehicles and motorcycles	3	5	262	769	89	1		5
G46	Wholesale trade, except of motor vehicles and motorcycles	13	27	1837	2719	228	4	1	51
G47	Retail trade, except of motor vehicles and motorcycles	12	21	554	2796	410	12		
H50	Water transport		1	303	126	1			3

For NPOs as per FATF definition, the risk in Luxembourg is driven by NPOs carrying out development and humanitarian projects abroad. As previously mentioned, this is a group known to have been exploited for TF purposes globally. Although the globally observed typologies have not been detected in relation to

Luxembourg NPOs developing projects abroad, this sub-sector remains highly vulnerable in view of the geography of their activities[368]**.** Whilst the RCS can track the entities registered as ASBL and *fondation*, there is no central taxonomy to classify their role/purpose. That said, most of them do not fall under the FATF definition of "NPO"[369]. In addition, the number of NPOs (ASBLs and *fondations*) falling within the FATF definition of NPO and engaged in activities abroad is relatively low. Among them, NPOs that engage in development and humanitarian projects abroad may apply to obtain a non-governmental organisation for development (DNGO) status from the Ministry of Foreign Affairs. In this case, they may obtain subsidies to increase the amounts of their projects though several programmes.

For additional detail on TF-related risks for NPOs, reference is made to the TF VRA and the ML/TF Vertical Risk Assessment Legal Persons and Legal Arrangements.

5.10.2. Legal arrangements

Luxembourg's legal arrangements sector can be sub-divided into domestic legal arrangements ("*fiducies*") and foreign trusts[370]. Luxembourg legislation defines ***fiducies*** under the Law of 27 July 2003 on trusts and fiduciary contracts ("2003 Trusts and Fiducies Law") and lists the *fiduciaires* that must comply with its provisions (article 4 of the 2003 Trusts and Fiducies Law). In line with the provisions set out in the 2003 Trusts and Fiducies Law, Luxembourg recognises **foreign trusts** according to the Hague Convention of 1 July 1985 on the Law applicable to trusts and on their recognition. The activity of professional trustee is mainly exercised by financial institutions.

As of 31 December 2023, there were 2,378 active *fiducies* and trusts registered with the *Registre des Fiducies et des Trusts*. 17.5% of trustees are natural persons and 82.5% are legal persons. None were residents of or domiciled in an in-scope country.

5.11. Cross-sector vulnerabilities

This section provides an overview of vulnerabilities with the potential to affect different sectors simultaneously, including newer and emerging vulnerabilities such as virtual assets and social media. These vulnerabilities should be carefully monitored by all stakeholders to reduce the risk of sanctions breach, non-implementation or evasion.

---

[368] Luxembourg, *Terrorist Financing Vertical Risk Assessment* ("Sectoral vulnerabilities"), 2022 (link)

[369] In 2020, the MoJ, in collaboration with the MoFA and the LBR, conducted an in-depth analysis of all types and status of Luxembourg NPOs in order to identify which NPOs are at risk of TF abuse and in order to compose the subset of NPOs that fall under the FATF definition (see Luxembourg, *Legal persons and legal arrangements vertical risk assessment* ("Non-profit organisations and terrorist financing"), 2022).

[370] As set out by the Law of 10 July 2020, "*a legal arrangement is considered to have a structure or functions similar to those of a trust and a trust when it enables a person to create legal relationships that place property under the control of a third party in the interest of a beneficiary or for a specified purpose and when it has the following characteristics: the property placed under the control of the third party constitutes a separate estate and does not form part of the estate of the third party; the title to the property placed under the control of the third party is established in the name of the third party or of another person on behalf of the third party; the third party is vested with the power and charged with the obligation, for which he or she is accountable, to administer, manage or dispose of the property placed under his or her control in accordance with the terms of the legal arrangement and the special rules imposed on the third party by law*".

5.11.1. Virtual assets

As access to the formal financial system has become increasingly closed to designated persons and entities via the introduction of various TFS, virtual assets (VAs) are becoming a means to evade sanctions.[371] VAs are globally considered as presenting material vulnerabilities given the pseudo-anonymity/anonymity they may afford and their potential to facilitate highly sophisticated forms of TFS evasion.

Several fundamental features of VAs mean they are exposed to risks associated with financial crime, including TFS non-implementation, evasion, or breach. These include the pseudo-anonymous/anonymous nature of virtual assets, the non-face-to-face business relationships involved, the international nature of the transactions, the increasing de-centralised nature of control over VAs, the volume of transactions, the speed of their execution, the irreversibility of these transactions and the technological complexity of VAs and VASPs[372]. This has enabled actors to employ sophisticated PF TFS evasion techniques using VA. For example, in one case referenced by the FATF, an actor used a digital version of layering to create thousands of transactions in real time through single-use VA wallets and then transferred funds instantaneously and nearly irreversibly across international borders[373].

The use of VAs has been linked to both DPRK and Iran. **For DPRK**, the RUSI identified three major areas where cryptocurrencies are being used in relation to PF: (1) to fundraise with the aim of converting into fiat currencies (e.g. cash) in the short term[374]; (2) to stockpile reserves of cryptocurrency to convert or spend at a future time; and (3) to circumnavigate explicit prohibited actions under international sanctions[375]. Whilst the final category is explicitly related to sanctions avoidance, the other two indirectly enable the circumvention of sanctions. The global scale of the DPRK's activity is reported to be significant. Indeed, some estimates suggest a stockpile in the region of hundreds of millions of dollars, generated through cyberattacks on exposed crypto exchange houses and opaque chain transactions whilst avoiding sanctions[376]. **Turning to Iran**, the state has previously announced its intention to develop and use a national digital currency[377] and announced in June 2024 that a pilot project would be launched in that respect[378]. Given the features of VAs described above, there is the potential that this could result in opaque and hard-to-trace transactions that pose a risk of TFS breach, non-implementation or evasion.

There is also evidence of state actors exploiting specific individuals to gain knowledge on how to evade or breach. For example, in September 2021, US citizen Virgil Griffith – a senior researcher at Ethereum Foundation (a non-profit supporting the Ether cryptocurrency) – pled guilty to providing technical advice to DPRK, including engaging in discussions "regarding using cryptocurrency technologies to evade sanctions and launder money"[379]. Links between the DPRK and a well-known hacker group active in VA theft have also been highlighted by the US Federal Bureau of Investigation (FBI)[380].

---

371 FATF, *Guidance on proliferation financing risk assessment and mitigation*, 2021 (link)

372 Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers,* 2020 (link)

373 FATF, *Guidance on proliferation financing risk assessment and mitigation*, 2021 (link)

374 It is noted that the methods by which DPKR then launders this money into fiat currency are still under investigation. Source: UN, *Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020)*, 2020 (link)

375 RUSI, *Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia*, 2019 (link)

376 Independent, *North Korea has amassed $670 million in bitcoin and other currencies through hacking,* 2019 (link); Nikkei Asia, *North Korea stole cryptocurrency via hacking: UN panel*, 2019 (link)

377 Foreign Policy, *Iran has a Bitcoin Strategy to beat Trump*, 2020 (link); Financial Tribune, *Iran to pilot national cryptocurrency*, 2021 (link)

378 Tehran Times, *Iran's central bank unveils CryptoRial*, 2024 (link)

379 US Department of Justice, *United States citizen pleads guilty to conspiring to assist North Korea in evading sanctions,* 2021 (link). See also: BBC, *Cryptocurrency expert admits aiding North Korea,* 2021 (link)

380 FBI press release, 2023 (link)

The use of VA to evade TF TFS is more challenging to assess as cases often contain classified national security information, but several examples have come to light, which suggest that this remains an important vulnerability globally. Recent estimates of global VA TF activity ranged from tens of thousands to millions of US dollars transferred annually[381, 382], though current figures are likely to be significantly higher. They also include cases where designated terrorist groups have allegedly run self-styled "fundraising campaigns" through virtual assets, for example by setting up multiple Bitcoin addresses for each potential donor in order to avoid funds being traced by law enforcement authorities[383,384]. These cases demonstrate the flexible and decentralized nature of VAs, which makes them a potentially useful mechanism for those looking to avoid TFS.

In Luxembourg, actors in the financial sector have been increasing their involvement regarding VAs, be it as provider or as customer, in recent years[385], which may expose them to a higher risk of TFS breach, non-implementation or evasion.

5.11.2. Cash

Globally, cash continues to be a prevalent aspect of terrorist operations[386] and has also been used by those seeking to evade PF TFS[387]. Cash smuggling is typically conducted through three main channels: (1) physical transportation by a natural person ("cash couriers"), (2) shipment through cargo, and (3) sending via mail[388] (cash couriers being the most common[389]). These mechanisms allow designated persons to move funds without encountering the AML/CFT safeguards established in financial institutions and provide a level of anonymity not offered by other forms of financial transaction. Whilst expensive relative to wire transfers, cash couriers rarely leave an audit trail and are particularly instrumental when seeking to move funds generated illegitimately. Even when cross border remittance of cash is prohibited, the origin and end use of cash can be unclear[390], limiting potential action by law enforcement. In almost all TF case studies included in a 2013 FATF report, cash was used and terrorist suspects were often in possession of significant amounts[391].

Vulnerabilities associated with physical movement of cash are most significant in economies with a high degree of cash usage, in countries where designated persons and entities are based, and at international ports and airports. Case studies show how cash couriering is frequently used to take funds into conflict zones where terrorist groups are active. This can be aided by "porous" national borders[392] and by the fact that amounts of funding often fall below cash declaration thresholds. For example, a cash declaration is required for amounts of EUR 10,000 or above entering/leaving the European Union: yet the level of funding of terrorist attacks in Europe has fallen below this amount[393].

With respect to PF TFS, UN PoE reports have highlighted the cooperation between DPRK and Iran in cash-smuggling activities via air travel. According to the UN Panel, officials of the DPRK based in Iran have been conducting cash transfers via air travel between Dubai and Teheran through diplomatic channels since

381 CoinDesk, *Palestinian Militant Group Has Received 3,370 Bitcoins in Donations Since 2015: Report*, 2020
382 New York Times, *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*, 2019
383 US Department of Justice, *Global disruption of three terror finance cyber-enabled campaigns*, 2020 (link)
384 New York Times, *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*, 2019 (link)
385 Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers,* 2020 (link)
386 FATF*, Emerging terrorist financing risks*, 2015 (link)
387 FATF, *FATF Guidance on Counter Proliferation Financing,* 2018 (link)
388 FATF, *FATF Recommendations* (*Recommendation 32: Cash couriers)*, accessed July 2025 (link)
389 FATF, *Money Laundering Through the Physical Transportation of Cash*, 2015 (link)
390 FATF, *Terrorist financing* (page 24), 2008 (link)
391 FATF, *Terrorist financing in West Africa*, 2013 (link)
392 FATF*, Emerging terrorist financing risks*, 2015 (link)
393 E. Oftedal (Norwegian Defence Research Establishment), *The financing of jihadi terrorist cells in* Europe, 2015 (link)

2009[394]. Additionally, UN PoE reports have noted the use of illicit ship-to-ship transfers as an increasingly advanced sanctions evasion technique by the DPRK. In several instances, illegal vessels were used as a means to transport undeclared cash and avoid sanctions[395]. They have also highlighted several cash withdrawal attempts from designated DPRK persons using personal and professional accounts based in countries such as China, Russia, Libya, Syria and the UAE[396].

Cash use in Europe has changed markedly as a result of the COVID-19 pandemic, but a significant degree of vulnerability remains. Data from ECB shows a material decline in the use of cash in day-to-day payments (cash lodged at central and commercial banks has fallen by 20-25% in the Euro area between March 2020 and March 2021)[397]. However, there has been a corresponding increase in demand for bank notes, suggesting that during the crisis people turned to cash as a tool to manage uncertainty[398]. This echoes data from FATF, which has continued to emphasize the challenges faced by AML/CFT authorities despite the increase in electronic payments during the pandemic[399].

The vulnerability of Luxembourg to the use of cash to evade TFS is relatively moderate. As a landlocked country in the center of Europe, Luxembourg is exposed to potentially significant cross-border movement of cash (particularly for amounts below the EU declaration limit). In previous years, it has also been suggested that the level of cash issuance in the country was at odds with perceived usage and outflows[400]. However, analysis in Luxembourg's 2020 NRA identified that the level of cash usage was in line with the Grand Duchy's share of both banking assets and debt securities issued. Moreover, recent increases in ATM withdrawals appear in line with the broader socio-economic landscape of Luxembourg (see the "Inherent Risk – Vulnerabilities" section of this report).

While the number of intra-EU cash declarations slightly decreased until 2022, with a minimal increase in 2023, the number of extra-EU declarations has increased since 2021. Since June 2021, cash disclosure is compulsory for unaccompanied cash following the entry into force of Regulation (EU) 2018/1672, which established an obligation to declare unaccompanied cash above EUR 10,000.

The total value in 2023 of declared and disclosed cash amounts to EUR 146.8 million[401]. Since the entry into force of Regulation (EU) 2018/1672, the ADA notes that cash disclosures are mainly submitted by financial institutions for extra-EU cash transport, leading to a higher declared overall value.

None of the countries which border Luxembourg is considered to be high-risk from a TFS perspective and, whilst some cash-intensive sectors operate in Luxembourg, there is only one casino operator.

With respect to the risks stemming from transactions, banking services and MVTS providers have put in place automatic transaction monitoring systems[402].

---

[394] UN Security Council, Panel of Experts report (page 48), 2020 (link)
[395] UN Security Council, Panel of Experts report (page 5), 2019 (link)
[396] UN Security Council, Panel of Experts report (page 55), 2021 (link)
[397] ECB, *Keynote speech by Fabio Panetta, Member of the Executive Board of the ECB, at the Deutsche Bundesbank's 5th International Cash Conference – "Cash in times of turmoil"*, 2021 (link)
[398] ECB, *Keynote speech by Fabio Panetta, Member of the Executive Board of the ECB, at the Deutsche Bundesbank's 5th International Cash Conference – "Cash in times of turmoil"*, 2021 (link)
[399] FATF, *COVID-19 Related Money Laundering and Terrorist Financing Risks*, 2020 (link)
[400] EUROPOL, *Cash is still king: Criminals prefer cash for money laundering,* 2015 (link)
[401] Data provided by the ADA for this risk assessment, 2023.
[402] Luxembourg, *Terrorist Financing Vertical Risk Assessment*, 2022

Table 16: Border cash declarations including cash disclosures (relating to currency and bearer negotiable instruments and as of 2021, commodities used as highly-liquid stores of value), 2018-2023, including both intra-EU and extra-EU cash transport[403]

		2018	2019	2020	2021	2022	2023
EU regulation[404]	Number of declarations	24	52	33	44	87	102
	Associated value (€)	736,724	1,168,759	2,240,335	1,789,554	57,448,104	161,748,572
National legislation[405]	Number of declarations	132	154	94	81	63	84
	Associated value (€)	4,677,049	16,328,960	5,657,768	3,220,514	16,363,697	14,755,516

5.11.3. Prepaid cards

Prepaid cards are defined as cards with "data encoded directly in the card, or stored remotely, that are preloaded with a fixed amount of electronic currency or value".[406] The global prepaid cards market is a dynamic and evolving field, with many different types of cards existing that have various product characteristics. Prepaid cards have evolved from the original "closed-loop" cards (i.e. gift certificates that allowed purchasing goods or services from a limited number of merchants) to "open-loop" cards that allow transactions with any merchant or service provider participating in the payment network and access to the global ATM network and cross-border payments, making them attractive for ML/TF purposes.[407] The use of prepaid cards has historically been linked to TF sanctions evasion as terrorists can obtain funds for terrorist activities in anonymous and unsuspicious ways.[408] For example, it was found that prepaid cards were used by terrorists in preparation of the November 2015 Paris attacks to purchase weapons and pay rental costs.[409]

While prepaid cards often have limits to their value, it is possible to use multiple cards at any one time by bundling them, which increases the risk of these cards being used in illicit activities, including TFS evasion. In addition, newer forms of prepaid cards that use cryptocurrencies are also emerging globally[410]. Such cards reduce the level of technical and financial knowledge required to convert (potentially illicit) VA into fiat money (cash), and therefore may increase the risk of sanctions breach, non-implementation or evasion.

Prepaid cards are not referenced in recent FATF guidance[411] as a means that can be used to evade sanctions, and there is no evidence globally that pre-paid cards are used to finance programmes of weapons of mass destruction. Luxembourg recognised new payment methods (including prepaid cards) as an emerging and evolving risk in the 2018 and 2020 NRA, including for TF.[412] In addition, it cannot be excluded that prepaid cards can be used to purchase dual-use items. In Luxembourg, customers can obtain prepaid gift cards, phone cards, cash vouchers, but also "open-loop" cards. However, the market for "open-loop" cards issued by banks in Luxembourg is limited: the largest issuer in Luxembourg stopped this activity some years ago. In

403 Table recreated based on Luxembourg, *National Risk Assessment* (page 143), 2020 (link), with data provided by ADA.
404 This refers to the obligation of declaration once the cash crosses the external border of the EU.
405 This refers to the obligation of declaration once the cash crosses an internal EU border.
406 FATF, *Emerging terrorist financing risks*, 2015 (link)
407 FATF, *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, 2013 (link)
408 FATF*, Emerging terrorist financing risks*, 2015 (link)
409 For example, see European Commission, *How the EU is combatting terrorist financing*, 2016 (link)
410 S&P Global, *Prepaid cards' dark underbelly hides potential financial sector pain*, 2020 (link)
411 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, 2021 (link)
412 Luxembourg, *National Risk Assessment* (page 74), 2020 (link)

2023, one bank stated that it provided prepaid cards to its clients, while no payment institution or electronic money institution issued prepaid cards as of December 2023. The level of risk related to TFS evasion for TF and PF in Luxembourg is therefore very limited.

5.11.4. Social media and crowdfunding

As outlined in several recent guidance documents, FATF has identified significant vulnerabilities associated with crowdfunding, social media and donations platforms – particularly related to TF (and therefore also TF TFS). This vulnerability is driven by "*anonymity, access to a wider range and number of potential sponsors or sympathisers, and the relative ease with which it integrates electronic payment mechanisms*"[413]. The use of encrypted communication channels adds to the vulnerability, as does the fact that online donors can often be unaware of the end-use of funds donated via social media and crowdfunding platforms (which in turn creates a risk of unwittingly financing designated actors).

A 2019 report from the Asia/Pacific Group on Money Laundering (APG) and the Middle East & North Africa Financial Action Task Force (MENAFATF) sets out three main types of social media and how they can be used for TF and/or to evade TFS, as laid out in the following table. Whilst the report is focused on TF, the framework used and typologies identified are also relevant for PF TFS more generally.

Table 17: Methods for terrorist misuse and abuse of social media types (as adapted from APG and MENAFATF report)[414]

Media type	Description	Examples of TF typologies identified in APG/MENA FATF report
Social networking and content hosting services (SNS and CHS)	• SNS "*allow users to create public or semipublic profiles and other content, articulate with other users they share a connection with and also view and interact with the content these other users have created*" • CHS "*allow users to create or upload content, for example, text, photos or videos, which is almost always public with less of a focus on connections/networks and more of a focus on general public consumption*"	• Services "*primarily used to solicit donations, promote terrorism through propaganda and radicalization*" • Services primarily used for social engineering in order to create false identities and avoid being flagged by sanctions monitoring institutions
Internet communications services (ICS)	• "*Allow two or multiple users to communicate in-real time over the internet normally in text but also in voice and video and with images*"	• Services "*used to privately communicate with campaigners or terrorist groups*" (note: primarily used to facilitate TF rather than actual financial transactions)

[413] FATF, *Emerging terrorist financing risks*, 2015 (link)

[414] APG and MENAFATF, *Social media and terrorism financing*, 2019 (link)

Media type	Description	Examples of TF typologies identified in APG/MENA FATF report
Crowdfunding services	• *"Allow users to fund a project, venture or cause within a bounded system by raising small amounts of money from many individuals"*	• Services used to fundraise for terrorist activities, *"with campaigners often disguising the use of funds for humanitarian causes"*

The EU SNRA has also identified risks of TFS evasion related to social media. The assessments identify and describe such a risk scenario, where crowdfunding platforms are created to collect funds for fictitious projects and transfer them abroad for ML purposes or to finance terrorist attacks. The associated TFS vulnerability is higher when the crowdfunding platform is unregulated and donation-based, as these platforms are outside the scope of financial institutions and of prudential and AML supervisors, and even higher if donations in VAs or (anonymous) electronic money are accepted[415].

UN PoE reports have also highlighted the use of social media and social engineering by the DPRK as means to run state-backed hacking campaigns. These hacking campaigns are primarily used as a means to generate revenue (through hacking MVTSs and VASPs to steal currency) but may leverage social media platforms to identify potential phishing targets and instigate contact[416]. One example includes the impersonation of human resources professionals at a business social media site, which was used to target employees and subsequently access classified data by sending email attachments with malware[417]. Social media is particularly vulnerable in this respect because social media firms do not consistently screen individuals against sanctions lists[418].

Vulnerability in Luxembourg relates primarily to the use of Luxembourg-based financial services by international crowdfunding providers. There are currently no major international Social Networking Services (SNS), Content Hosting Services (CHS) or Internet Communications Services (ICS) headquartered in Luxembourg; however, most international providers operate within the country. Of the three social media types, the most material TFS vulnerability for Luxembourg stems from financial services offered to global crowdfunding services. While the overall crowdfunding market in Luxembourg is small (so far no crowdfunding service provider, within the meaning of the European Crowdfunding Regulation, has been licensed in Luxembourg), crowdfunding typically uses to a significant extent payment methods such as bank transfers, credit and debit cards, and internet payment services. Those services are offered by banks and MVTS providers, which have a large presence in Luxembourg.

5.11.5. Vulnerabilities related to the maritime sector

While export sanctions are not in scope of this report, maritime vessels can be the subject of TFS and deceptive shipping practices can be a method of indirect TFS evasion. According to FATF, direct exploitation of the sector relates to (1) delivering components and materials for use in WMD or their delivery systems and (2) illicitly engaging in economic sectors that generate revenue, which can provide the underlying finance

[415] European Commission, *Supranational risk assessment*, 2019 (link)

[416] UN, *Midterm report of the Panel of Experts submitted pursuant to resolution 2569 (2021)* (page 50), 2021 (link)

[417] UN, *Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)* (pages 48-49), 2021 (link)

[418] RUSI, *Social Media and Terrorist Financing What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?*, 2019 (link)

for a WMD programme.[419] In May 2020, the US Department of State, the US Department of the Treasury and the United States Coast Guard issued guidance on sanctionable or illicit shipping sanctions evasion.[420] They noted that "*malign actors constantly seek novel ways to exploit global supply chains for their benefit*" and outlined several tactics used to facilitate illicit maritime trade that include:[421]

- Disabling or manipulating the Automatic Identification System (AIS) on vessels
- Physically altering vessel identification
- Falsifying cargo and vessel documents
- Ship-to-ship transfers
- Voyage irregularities
- False flags and flag hopping
- Complex ownership or management

Any of the above methods (used singularly or in conjunction with others) that engage a sanctioned vessel in financial transactions or activities relating to economic resources are thus considered as TFS evasion techniques. For example, complex legal structures could be used to disguise the ultimate beneficial owner of a ship's cargo in combination with falsified ship vessel documents[422].

There is evidence that DPRK continues to operate sanctioned ships and to engage in sanctions-evasion techniques related to the shipping industry. For example, in September 2021, the UK conducted operations in the East China Sea, detecting ships acting in suspected breach of UN sanctions against DPRK[423]. In addition, DPRK has also been identified as conducting illicit ship-to-ship transfers of cargo at sea to import refined petroleum products that contribute to the country's nuclear and ballistic missile programmes[424]. While DPRK frequently uses foreign flags on ships, vessels can be owned by trading companies or unknown parties located in other nations[425].

The maritime sector has been identified as a cross-sector vulnerability because of its close links to other sectors that could in turn be used to (indirectly) evade PF TFS. Maritime insurance and re-insurance is one such example (see "Inherent Risk – Vulnerabilities" section for details on Insurance sector). Correspondent banking services are exposed to a similar type of risk and other cross-sector vulnerabilities can relate to entities such as trading companies and port authorities. Exposure is typically higher in countries that have a large shipping industry and/or a significant maritime (re)insurance market and/or a banking hub for maritime clients.

FATF's guidance highlights several risk factors, which may indicate sanctions evasion related to the maritime sector. These largely relate to inconsistencies in shipment type, freight and ship documentation, destination and shipping routes and are summarised below.

---

[419] FATF, *Guidance on proliferation financing risk assessment and mitigation*, 2021 (link)

[420] The guidance indicates "a focus on Iran, North Korea and Syria" and has a wider scope than that covered in this report. See: US Treasury, *Guidance to address illicit shipping and sanctions evasion practices*, 2020 (link)

[421] United States Coast Guard, *Guidance to Address Illicit Shipping and Sanctions Evasion Practices*, 2020 (link)

[422] United States Coast Guard, *Guidance to Address Illicit Shipping and Sanctions Evasion Practices*, 2020 (link)

[423] UK, *UK conducts UN sanctions enforcement to counter North Korea's weapons programmes*, 2021 (link)

[424] UN Security Council, *Final report of the Panel of Experts submitted pursuant to resolution 2464 (2019)* (page 7), 2020 (link)

[425] Foundation for Defense of Democracies, *UN Report Reveals North Korea's Persistent and Evolving Maritime Sanctions Evasion Schemes,* 2020 (link)

Table 18: Risk indicators related to the maritime sector (adapted from 2021 FATF Guidance)[426]

• Trade entity is registered at address likely to be a mass registration address (e.g. high-density residential buildings, post-box addresses, commercial buildings) • Person or entity preparing shipment lists a freight forwarding firm as final destination • Destination of a shipment is different from importer's location • Inconsistencies are identified across contracts, invoices, or other trade documents (e.g. contradictions between name of the exporting entity and the name of the recipient) • Shipped goods have a low declared value vis-à-vis the shipping cost • Shipment of goods is incompatible with the technical level of country where shipped (e.g. semiconductor manufacturing equipment shipped to country with no electronics industry) • Shipment of goods is made in a circuitous fashion (e.g. multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping) • Shipment of goods is inconsistent with normal geographic trade patterns (e.g. the destination country does not normally export or import the goods listed in trade transaction documents) • Shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards, export control laws or weak enforcement • Payment for imported commodities is made by entity other than consignee of the commodities with no clear economic reasons (e.g. by a shell or front company)

Despite being a landlocked country, Luxembourg's emerging maritime business ecosystem means the country may face some exposure to risk of TFS non-implementation, evasion or breach. It is estimated that more than 200 ships fly the Luxembourg flag[427]. In addition, Luxembourg is also home to three protection and indemnity (P&I) clubs[428], with the third having started its activity in 2021. One of these clubs issued a circular in 2019 which highlighted the risks related to DPRK and to sanctions non-implementation, evasion or breach.

5.11.6. Dual-use items

Dual-use items (goods and technology) have both civil and military applications. Examples range from raw materials and components (e.g. aluminum alloys, bearings) to complete systems (e.g. lasers). They also include items that could be used in the production or development of weapons of mass destruction (WMD) or military goods, chemical manufacturing equipment, or machine tools. The export of such items is regulated through export control laws and regulations[429] (albeit these are not considered in this risk assessment).

The nature of dual-use items makes them particularly subject to risks of PF TFS evasion and actors can be involved directly or indirectly across different stages of the PF value chain[430]. Risks of direct involvement in PF are higher in countries that are major military manufacturers/suppliers, as well as in those producing dual-use items. In such countries, many industrial sectors can be exposed to PF TFS risks, for example

[426] FATF, *Guidance on proliferation financing risk assessment and mitigation*, 2021 (link)

[427] *Maritime Sector: Luxembourg, a Maritime Alternative*, accessed September 2024 (link)

[428] Protection and indemnity insurance, more commonly known as P&I insurance, is a form of mutual maritime insurance provided by a P&I club.

[429] UN Security Council Resolution 1540 (2004); Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items; Law of 27 June 2018 & Grand Ducal Regulation of 14 December 2018.

[430] PF value chain is defined as: (1) raising funds, (2) moving or obscuring funds; and (3) using funds (procurement). Direct financing can be thought of as an activity which directly contributes to the development of nuclear capability, such as providing funding to a state nuclear agency or procurement of dual-use items. Indirect financing can be considered as activity where there are more steps between finance and the proliferating actor. Further details are provided in the "Introduction" of this report. See also: Centre for New American Security, *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation,* 2018 (link)

producers of everyday items for the commercial industry (e.g. electronic components, carbon fibre, chemicals) as well as those in the financial services sector (e.g. by providing bank accounts, loans, and export financing to firms associated with dual-use items). For example, the UK's PF risk assessment cites the case of a company that provided internet banking services to a government shipping agency which allowed a state actor to import dual-use items in breach of sanctions requirements[431]. Risks of indirect PF concern situations where there are several steps between finance and the proliferating actor.

In Luxembourg, the cross-sector vulnerability related to dual-use items exports is relatively limited and, where it exists, is linked to indirect involvement in TFS breach, non-implementation or evasion. Luxembourg does not have a significant dual-use or military industry, and its economy is orientated primarily towards financial services rather than manufacturing. Accordingly, a relatively small number of individual licenses[432] have been granted by OCEIT related to export of items subject to controls (see table below)[433]. Direct involvement in TFS evasion (e.g. providing financial products directly to a dual-use goods related entity circumventing TFS) is therefore less likely. Potential exposure is more likely to come from the provision of services (e.g. by TCSPs) to an entity involved in dual-use goods which evades TFS (e.g. set-up of complex networks of companies designed to mask the end recipient of funds). Here, the significant size of Luxembourg's TCSP sector may create a vulnerability[434]. See "Specialized PFS" in "Inherent Risk – Vulnerabilities" for more details.

Table 19: Export licenses granted by OCEIT for all third countries, 2018-2023

		Dual use items	Military items
2018	Number of licenses	106	7
	Value	€3,701,000	€85,266
2019	Number of licenses	160	16
	Value	€773,000	€3,556,535
2020	Number of licenses	94	11
	Value	€6,186,000	€9,701,836
2021	Number of licenses	73	3
	Value	€7,580,000	€31,378,879
2022	Number of licenses	66	23
	Value	€7,445,000	€3,694,521
2023	Number of licenses	56	14
	Value	€5,135,000	€3,832,849

[431] UK, *National Risk Assessment of Proliferation Financing* (pages 4 and 5), 2021 (link)

[432] This statistic excludes global licenses, which are not permitted for sensitive goods and/or countries. For additional detail, please refer to the mitigating factors described in the section on OCEIT.

[433] OCEIT internal data.

[434] For example, out of a total of 100 Specialised PFSs supervised by the CSSF in 2023, 85 performed TCSP activities. The latter have 6,428 employees, a balance sheet of €1.02 billion and a profit of €90 million.

6. Mitigating Factors

Luxembourgish entities mitigate against PF and TF by complying with UNSCR- and EU-mandated sanctions, as well as Luxembourg-specific sanctions if any. There are also specific controls on proliferation-sensitive items and on exports to countries that may be exposed to PF or TF.

Since the entry into force of the Law of 19 December 2020 on the implementation of restrictive measures in financial matters, as modified (the "Law of 19 December 2020"), UN sanctions are automatically transposed in Luxembourg. Upon identification of a positive match, operators are obliged to freeze funds without delay, freezing being defined as "*any action to prevent any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character, destination or other change that would enable the use of the funds, including portfolio management*"[435].

Luxembourg authorities work together as required – both bilaterally and in the context of the Monitoring Committee on International Financial Sanctions – as well as with the operators (i.e. the natural and legal persons who are required by law to implement the restrictive measures) to identify funds or other assets of designated persons and entities and those acting on their behalf or at their direction and ensure that such persons and entities are prevented from operating or from executing financial transactions related to such funds.

This section explores Luxembourg's sanctions landscape further, detailing specific mitigating factors taken by key authorities and public agencies, including supervisors, to mitigate the risk of PF and TF in their sectors.

6.1. Legal framework

The Law of 19 December 2020 establishes the legal basis for the implementation by Luxembourg of financial sanctions (also referred to as "restrictive measures") adopted against certain states, natural and legal persons, entities and groups[436]. The Law was established to further enhance the framework of sanctions implementation in Luxembourg, whilst retaining elements of the framework created by the previous law of 27 October 2010. The following table provides more context on the scope and applicability of TFS, as set out in the Law of 19 December 2020.

[435] Article 2, Law of 19 December 2020 (link)

[436] The Law of 19 December 2020 replaces the Law of 27 October 2010 and lays out among others enhanced scope and applicability for financial sanctions.

Table 20: Scope and applicability of TFS in Luxembourg

Scope of TFS/financial restrictive measures	Applicability of TFS/financial restrictive measures
• "Restrictive measures in financial matters" means: – *"The prohibition or restriction of financial activities of any kind"* – *"The prohibition or restriction on the provision of financial services, technical assistance, training or advice in relation to a State, natural or legal person, entity or group referred to in this law; or"* – *"The freezing of funds, assets or other economic resources owned or controlled, directly, indirectly or jointly, with or by a person, entity or group referred to in this law or by a person acting on their behalf or at their direction"*[437]	In Luxembourg, restrictive measures apply to: a. *"natural persons of Luxembourg nationality who reside or operate in or from the territory of the Grand Duchy of Luxembourg or abroad"* b. *"Legal persons having their registered office, a permanent establishment or their centre of main interests on the territory of the Grand Duchy of Luxembourg or abroad"* c. *"Branches of Luxembourg legal persons established abroad and branches in the Grand Duchy of Luxembourg of foreign legal persons"* and d. *"All other natural and legal persons operating on the territory of the Grand Duchy of Luxembourg"*[438]

One of the key features of the Law of 19 December 2020 is the automatic transposition of UN sanctions lists[439,440]. Grand-Ducal regulations may also impose additional restrictive measures/TFS "*pending the formal adoption of decisions within the United Nations Organisation or the European Union*"[441] for up to 60 days with a possibility to extend the adopted measure each time for 30 days. Failure to comply with applicable restrictive measures also constitutes an associated predicate offense of money laundering under the Criminal Code[442].

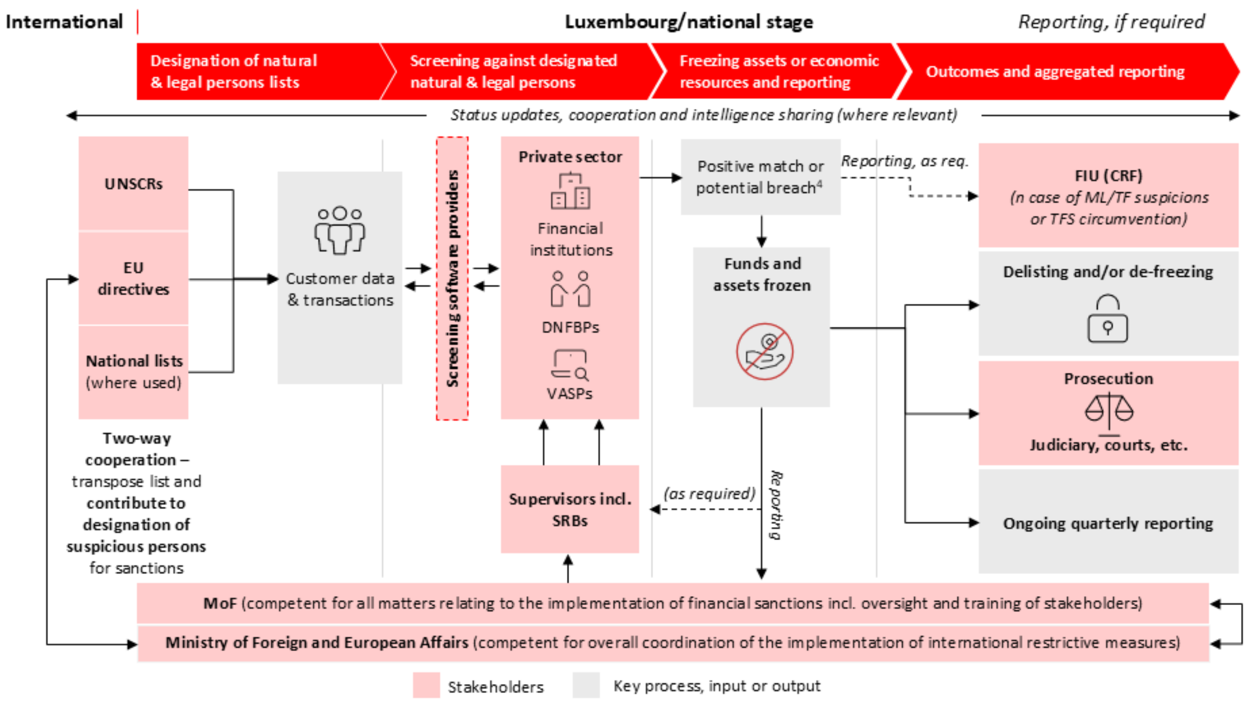
6.1.1. High-level process for the implementation of TFS

The implementation of TFS in Luxembourg is understood as a four-step process involving a series of stakeholders, as well as several inputs, outputs and processes. These steps span across the financial sector and the non-financial sector and involve a series of stakeholders with varying degrees of involvement. Figure 5 provides a simplified view of these four steps, which are:

- Designation of natural & legal person lists
- Screening against designated natural & legal persons
- Freezing assets or economic resources and reporting
- Outcomes and aggregated reporting

437 Article 2, Law of 19 December 2020 (link)
438 Article 3, Law of 19 December 2020 (link)
439 Article 4, Law of 19 December 2020 (link)
440 Article 1 of Grand-Ducal Regulation of 14 November 2022 provides that operators are to implement restrictive measures without delay and without prior notification (link).
441 Article 5, Law of 19 December 2020 (link)
442 Article 5, Law of 20 July 2022 (link)

Figure 5: Luxembourg sanctions process flow



The first step of the sanctions application process is the **designation of natural and legal persons lists**. As per the Law of 19 December 2020, designations at UN level and EU level are automatically and directly applicable in Luxembourg.

The second stage involves **screening against designated natural & legal persons.** Most commonly, screening is done in large volumes via support from specialised software tools/sanctions screening solutions providers. It is conducted both by private sector organisations and by supervisors/SRBs (e.g. at market entry and on an ongoing basis afterwards). Smaller operators (e.g. DNFBPs) may carry out manual checks. Throughout this process, the Ministry of Finance offers guidance and support, frequently responding to ad hoc requests and helping operators to understand their obligations.

Thirdly, if a **positive match or breach** is uncovered, operators are required to **freeze funds**[443] **and economic resources**[444] immediately[445]. Once frozen, operators must report "*without delay*" to the Ministry of Finance[446]. In a situation of homonyms, if, after gathering identifiers, it can be clearly demonstrated that two individuals are not the same person, the Ministry of Finance need not be contacted[447]. However, in case of any doubt, the Ministry of Finance should still be contacted, and operators are expected to suspend any

---

[443] In accordance with the Law of 19 December 2020 (Article 2), freezing of funds refers to "*any action to prevent any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character, destination or other change that would enable the use of the funds, including portfolio management*".

[444] In accordance with the Law of 19 December 2020 (Article 2), freezing of economic resources refers to "*any action intended to prevent the use of economic resources to obtain funds, goods or services of any kind, including the selling, hiring or mortgaging of such funds, goods or services*".

[445] Article 1, Grand-Ducal Regulation of 14 November 2022 (link)

[446] Article 6, Law of 19 December 2020 and Article 2, Grand Ducal Regulation of 14 November 2022

[447] Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals* (page 31), 2021 (link)

transactions on the account until the situation is clarified[448]. Whenever there is a true positive sanctions screening match which also triggers ML/TF suspicions[449], or in cases of failure to comply with restrictive measures as provided for by article 10 of the Law of 19 December 2020, a report must be filed to the CRF[450].

Meanwhile supervisors oversee activities in their area of competence (e.g. ensuring supervised professionals/entities fulfil their obligations when conducting onsite inspections), with the Law of 19 December 2020 granting powers consistent with the 2004 AML/CFT Law to intervene or investigate non-compliance[451]. As well as continuing to support operators during this stage, the Ministry of Finance also acts as an advisory body for operators and supervisors.

Lastly, the final stage is **outcomes and aggregated reporting**. Operators are expected to complete quarterly inventories of frozen assets. The Ministry of Finance consolidates operators' reports and shares this with the European Commission on a regular basis.

The last possible outcome is de-listing (e.g. where an individual or entity is removed from a TFS list) and de-freezing (e.g. based on authorisations, following a de-listing, etc.). For de-listings, the process depends on the sanctioning body, but Luxembourg may submit de-listing requests on residents' or citizens' behalf to the UN or submit de-listing request for entities to the EU[452,453]. In exceptional cases, and where the exemption conditions are met, the Minister of Finance can also issue "*authorisations derogating from the prohibitions and restrictive measures*"[454]. Individuals can also submit their de-listing request directly. The Ministry of Finance's website[455] provides information to direct persons and entities to submit de-listing requests. For applications against an EU regulation, an application for the annulment of an act imposing financial restrictive measures is heard in the General Court of the EU[456]. An application for the annulment of an act imposing financial restrictive measures following a designation under the national regulation is heard in the Tribunal Administratif[457]. The Ministry of Finance publishes de-listing decisions in the Official Gazette and on its website. The Ministry of Finance also communicates de-listing decisions via its newsletter.

6.2. Overview of roles & responsibilities

There are several stakeholders involved in the implementation of financial sanctions in Luxembourg, with different roles and degrees of involvement. This includes ministries (Ministry of Finance, Ministry of Justice, Ministry of Foreign and European Affairs), national supervisors (CSSF, CAA, AED), the financial intelligence unit (CRF), self-regulatory bodies (OEC, IRE, OAL/OAD, CdN, CdH) and other agencies/administrators (ADA, LBR). Whilst, at the time of writing, no prosecutions related to TFS have occurred in Luxembourg, law enforcement entities (prosecution authorities, investigative judges, the Judicial police service) may take

448 Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals* (page 31), 2021 (link)

449 Law of 20 July 2022 (link)

450 This obligation derives from the Law of 12 November 2004, as amended, which states that reporting occurs where operators "*have reasonable grounds to suspect that money laundering, an associated predicate offence or terrorist financing*" is being committed or has been committed.

451 Article 6, Law of 19 December 2020 (link)

452 Global Investigations Review, *The Guide to Sanctions - EU Restrictive Measures*, 2021 (link)

453 EU Council, *Restrictive measures (Sanctions) - Update of the EU Best Practices for the effective implementation of restrictive measures*, 2018 (link)

454 Law of 19 December 2020 (link)

455 Website of the Ministry of Finance (link)

456 Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals* (page 14), 2021 (link)

457 Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals* (page 15), 2021 (link)

action as required. The table below sets out the roles & responsibilities of core stakeholders, as defined in key documentation/laws, with the subsequent sections providing additional detail on each.

Table 21: Stakeholders involved in the implementation of TFS relating to TF and PF in Luxembourg

Stakeholder	Key responsibilities related to TFS for PF and TF
Ministries	
Ministry of Finance	• Competent authority for all matters relating to the implementation of financial sanctions • "The Minister responsible for Finance is also competent to exceptionally issue authorisations derogating from the prohibitions and restrictive measures imposed if the resolutions and acts referred to in Article 1 allow such derogations and under the conditions provided for therein"[458]
Ministry of Foreign Affairs	• Competent for "coordination with regard to the implementation of international sanctions"[459] • The Minister for Foreign and European Affairs, Defence, Development Cooperation and Foreign Trade "is designated as the competent authority to communicate to the United Nations Sanctions Committees the natural and legal persons, entities and groups to which the restrictive measures in financial matters apply, as well as all information relating thereto, for the purpose of their inclusion on the United Nations Consolidated List"[460]
Ministry of Justice	• Has no specific competencies related to TFS, but competent for matters regarding FATF[461] • Has indirect responsibilities related to CFT
Supervisors and SRBs	
Commission de Surveillance du Secteur Financier (CSSF)	• Responsible for "prudential, AML/CFT including TFS supervision of professionals of the financial sector falling under the scope of its competences". On the basis of Article 33 of CSSF Regulation no. 12-02, these persons are required i.a. to keep the CSSF informed when States, natural and legal persons, entities or groups involved in a transaction or business relationship subject to prohibitions or restrictive measures in financial matters are identified"[462] • "Has the same powers as those conferred by Articles 8-2, 8-4, 8-5, 8-6, 8-7 and 8-9 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended"[463]
Commissariat aux Assurances (CAA)	• "Responsible for the supervision of natural and legal persons falling within its competence in the insurance sector for the purposes of the implementation of the Law of 19 December 2020 on the implementation of restrictive measures in financial matters"[464]. In accordance with the combined provisions of article 2, paragraph 2, and article 31 of the CAA Regulation 20/03 dated 30 July 2020 on the fight against money laundering and terrorism financing, these persons have to apply restrictive measures and inform without delay the competent authorities in financial sanctions matters. A copy of this reporting has to be addressed to the CAA.

[458] Article 6, Law of 19 December 2020 (link)
[459] Grand-Ducal decree of May 28, 2019 establishing the ministries (link)
[460] Article 7, Law of 19 December 2020 (link)
[461] Grand-Ducal decree of May 28, 2019 establishing the ministries (link)
[462] Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals*, 2021 (link)
[463] Article 6, Law of 19 December 2020 (link)
[464] Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals*, 2021 (link)

<table>
<tr><th>Stakeholder</th><th>Key responsibilities related to TFS for PF and TF</th></tr>
<tr><td></td><td>“Has the same powers as those conferred by Articles 8-2, 8-4, 8-5, 8-6, 8-7 and 8-9 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended”[465]</td></tr>
<tr><td>Administration de l'Enregistrement et des Domaines (AED)</td><td>“Responsible for the supervision of specific categories of persons referred to in art. 1 of the Law of 10 August 2018”[466]
“Has the same powers as those conferred by Articles 8-2, 8-4, 8-5, 8-6, 8-7 and 8-9 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended”[467]</td></tr>
<tr><td>Self-regulatory bodies (SRBs): OAL/OAD, CdN, OEC, IRE, CdH</td><td>Responsible for the supervision of professionals within their respective competencies
“[Have] the same powers as those attributed to them by Articles 8-2a, 8-10, 8-11, 8-12 and 8-13 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended”[468]</td></tr>
<tr><td colspan="2">Other authorities/administrators</td></tr>
<tr><td>Office du contrôle des exportations, importations et du transit (OCEIT)</td><td>“Competent authority for issuing authorizations for transactions such as the export, transfer, transit, technical assistance, brokering, and import of listed defense-related items, dual-use items and torture-related items; also grants derogatory authorizations for items of a strictly civilian nature within the framework of economic restrictive measures; the Political Affairs Directorate further has co-decision power concerning export autorisation for dual-use items and defense-related items”[469]
Has no specific competencies related to TFS for PF and TF</td></tr>
<tr><td>Administration des Douanes et Accises (ADA)</td><td>“Competent authority for the control of the physical transport of cash entering or leaving the Grand Duchy of Luxembourg as well as for the control of cash entering or leaving the Union”[470]
Competent authority for the levy of customs and excise duties</td></tr>
<tr><td>Luxembourg Business Registers (LBR)</td><td>Mission to “manage and to develop the different registers it may be entrusted with by law, under the authority of the Minister of Justice”[471], including:
- RCS (since 23 January 2003)
- RESA (since 1 June 2016)
- RBE (since 13 January 2019)</td></tr>
<tr><td colspan="2">Judiciary authorities and law enforcement agencies</td></tr>
<tr><td>Financial Intelligence Unit (FIU)/Cellule de Renseignement Financier (CRF)</td><td>The 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 money laundering (ML), associated predicate offences or terrorist financing (TF).
In particular, it receives and analyses:
- Suspicious transaction and activity reports transmitted by a professional subject to the AML/CFT legislation as provided by article 5, paragraph 1, a) of the 2004 AML/CFT Law; and
- Information communicated by other AML/CFT competent authorities pursuant to article 74-2 (4) of the amended law of 7 March 1980 on the judiciary organisation.</td></tr>
</table>

465 Article 6, Law of 19 December 2020 (link)
466 Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals*, 2021 (link)
467 Article 6, Law of 19 December 2020 (link)
468 Article 6, Law of 19 December 2020 (link)
469 Provided by OCEIT.
470 Law of 16 July 2021 (link)
471 Website of LBR (link)

Stakeholder	Key responsibilities related to TFS for PF and TF
	• The CRF disseminates, spontaneously and upon request, the results of its analysis and any other relevant information when there are reasonable grounds to suspect money laundering, 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. • 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.
Prosecution authorities	• Conduct all necessary actions to investigate and prosecute criminal offenses and recover crime-related assets[472]
Investigative Judges (*Juges d'instruction*)	• Order measures that restrict individual freedoms (i.e. coercive measures) such as provisional detention, searches and seizures[473]
Judiciary police (*Service de Police Judiciaire*, SPJ)	• Carry out "research and investigations in relation to more serious offenses or of particular complexity"[474], including economic and financial crime
Private sector	
Private sector operators (e.g. DNFPBs, FIs…)	• Freeze and report "without delay" and without prior notice funds (defined as "financial assets and economic advantages of any kind") where a positive match is identified, and report this to Ministry of Finance

The following sections deep-dive into each of the above stakeholders as part of the counter-TF/counter-PF regime.

6.3. Ministries

6.3.1. Ministry of Finance

Stakeholder	Key responsibilities related to TFS for PF and TF
Ministries	
Ministry of Finance	• Competent authority for all matters relating to the implementation of financial sanctions • "The Minister responsible for Finance is also competent to exceptionally issue authorisations derogating from the prohibitions and restrictive measures imposed if the resolutions and acts referred to in Article 1 of the Law of 19 December 2020 allow such derogations and under the conditions provided for therein"[475]

[472] Luxembourg, *National Risk Assessment,* 2020

[473] Luxembourg, *National Risk Assessment,* 2020

[474] Judicial Police Service's (SPJ) webpage, accessed July 2025 (link)

[475] Article 6, Law of 19 December 2020 (link)

6.3.1.1. Overview of competencies

The Minister of Finance is competent to "*deal with matters relating to the enforcement of financial restrictive measures on the part of the natural and legal persons, entities and groups concerned, as well as on the part of the natural and legal persons obliged to apply them*[476]".

This competence includes:

a. Dealing with any questions regarding the implementation of financial restrictive measures from the persons, entities and groups targeted, as well as from natural and legal persons called upon to apply them, and dealing with any related disputes;
b. Dealing with any questions and disputes regarding homonyms;
c. Dealing with any questions and disputes regarding unintended consequences of the financial restrictive measures on assets;
d. Exceptionally granting authorisations exempting from the imposed prohibitions and financial restrictive measure in line with applicable legal provisions.

In addition, the Ministry of Finance provides information via its newsletter and its website on the implementation of prohibitions and restrictive measures.

In its role as competent authority in matters of implementation of financial sanctions, the Ministry of Finance does not substitute itself to the supervisory authorities or the self-regulated bodies in the carrying-out of their supervisory tasks. In this respect, the Ministry does not carry out on-site inspections or other similar controls of the supervised entities, leaving this to the competent authorities (including SRBs).

6.3.1.2. Information/awareness raising on TFS

The Ministry of Finance's website[477] is the primary source of information for natural and legal persons who are required to implement TFS in Luxembourg, both on general obligations and practical guidance relating to TFS implementation. Originally created with a focus on TF-TFS, the Ministry of Finance's website now covers all financial sanctions regimes applicable in Luxembourg. Amongst others, it provides information on the applicable sanctions regimes for Iran and DPRK, as well as the FATF guidance on PF.[478] The website is available both in the English and French languages.

In the context of its role as competent authority, the Ministry of Finance also issues guidelines related to the implementation of financial sanctions. One set of guidelines deals specifically with financial sanctions in the framework of TF, whereas a second set relates to implementation of financial sanctions against third countries, entities or individuals (including also PF-TFS). Both sets are available in English and French on the Ministry of Finance's website.[479]

In addition, the Ministry of Finance also manages a newsletter (the "Newsletter"), which is available to all operators free of charge. Same as for the website, the Newsletter originally aimed to provide information to economic operators on TF-related designations. It has since expanded to a publication that informs operators on all matters relating to financial sanctions, irrespective of sanctions regime(s), and had more than 2,300 subscribers at the end of 2023. At present, the Newsletter is published on an ad hoc basis, i.e. every time there is a designation or a removal of designation as well as whenever the validity of a sanctions regime is extended. It is also published to refer to documents that may be of interest in the context of TFS, such as,

[476] Article 6, Law of 19 December 2020 (link)
[477] Section on international financial sanctions on the website of the Ministry of Finance, accessed July 2025 (link)
[478] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, 2021 (link)
[479] Section on international financial sanctions on the website of the Ministry of Finance, accessed July 2025 (link)

for example, opinions of the EU Commission, publication of guidelines or other relevant documents and information.

Furthermore, since 2019 and following requests from other authorities/economic operators, the Ministry of Finance participates as well in awareness-raising activities. These include thematic conferences and other industry-related events related to financial sanctions implementation, in coordination with other authorities. For example, in 2019-2020, the Ministry of Finance participated in four conferences dealing with the matter of financial sanctions. The conferences included presentations and discussions on topics relevant for all regimes of TFS, such as authorization requests, good practices, red flags ("dos and don'ts") as well as information on the legal and regulatory framework. After the adoption of the Law of 19 December 2020, the Ministry of Finance participated in conferences focusing on providing information and clarifications about the new legal framework and in additional events in order to maintain and increase its outreach towards other authorities and operators in matters of TFS.

6.3.1.3. Operator outreach

The Ministry of Finance organizes or otherwise actively supports frequent outreach to the operators. In addition to the website and the Newsletter, such outreach takes mainly the form of bilateral meetings with the operators wishing to discuss specific files, in particular before or during the authorization request process. Bilateral contacts take place regularly with the competent authorities too and cover a large range of subjects in relation to TFS, from exchange of intelligence amongst authorities to requests for exemption to the applicable freezes as per the current legislative framework and cases of negative press on specific persons/entities that are nevertheless not listed. In addition to clarifying queries on matters of implementation of TFS, these contacts, both with other authorities as well as with operators, facilitate identification of funds and assets falling under the scope of TFS and can therefore enhance the prevention efforts of the authorities across the national spectrum.

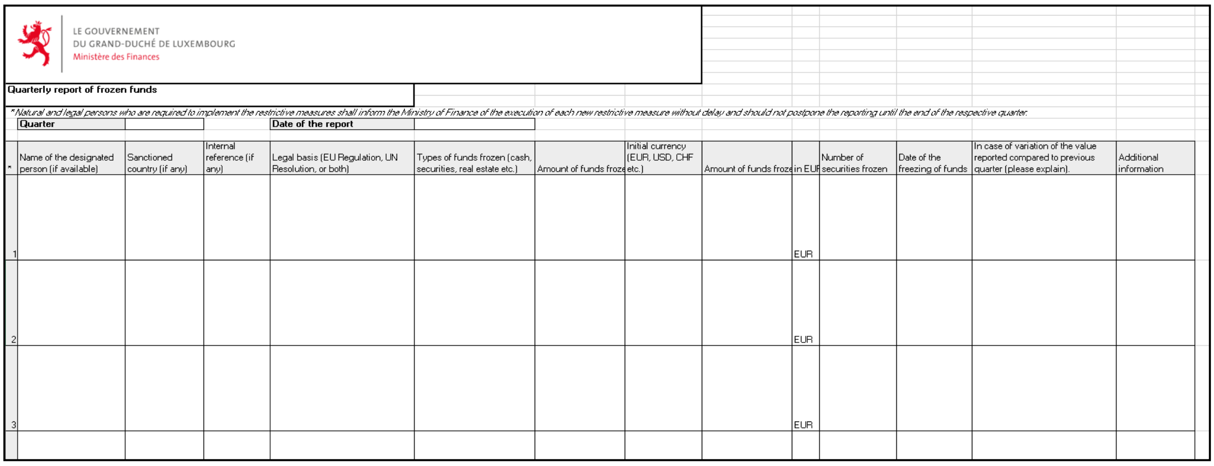
More generally, the Ministry of Finance is available to support operators in the fulfilment of their obligations. Whilst formal requests/those sent in writing are recorded, communications may also be conducted in a more informal manner (e.g. over conference calls). Comments and questions are regularly received, with banks producing the greatest number of requests. Generally speaking, most cases of frozen assets start with an inquiry about the sanctions regime, obligations and reporting formats. When needed, the Ministry of Finance shares relevant information with supervisors.

6.3.1.4. Collation of reports

Upon the identification of a match with a sanctioned person, operators are obliged to freeze assets and report it without delay to the Ministry of Finance. Alongside reporting new asset freezes without delay, operators who have frozen assets (irrespective of their sector/business type) must also provide a quarterly inventory on the status of frozen assets to the Ministry of Finance.

Previously, the method used to submit reports (both initial reporting and quarterly inventory) varied by operator, with some choosing to use Excel files and others preferring emails or PDF documents. Since Q2 2021, the Ministry of Finance has a standardized Excel reporting template, which is used to streamline the reporting process. The template also includes a section, where relevant, to explain any variation in asset value since the previous quarter (e.g. market value fluctuations, currency exchange rate fluctuations, fees charged under authorisation, etc.).

Figure 6: Excerpt of quarterly reporting template to Ministry of Finance


LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Finances

Quarterly report of frozen funds

*Natural and legal persons who are required to implement the restrictive measures shall inform the Ministry of Finance of the execution of each new restrictive measure without delay and should not postpone the reporting until the end of the respective quarter.

Quarter | Date of the report

*	Name of the designated person (if available)	Sanctioned country (if any)	Internal reference (if any)	Legal basis (EU Regulation, UN Resolution, or both)	Types of funds frozen (cash, securities, real estate etc.)	Amount of funds froze	Initial currency (EUR, USD, CHF etc.)	Amount of funds froze	in EUR	Number of securities frozen	Date of the freezing of funds	In case of variation of the value reported compared to previous quarter (please explain).	Additional information
1									EUR				
2									EUR				
3									EUR				

The Ministry of Finance collates and aggregates these reports, sharing information with the European Commission as required. The table below captures the total value of frozen assets in each year.

Table 22: Total value of frozen assets for in-scope countries, 2018-2023 (as reported to the Ministry of Finance)[480]

	2018	2019	2020	2021	2022	2023
Total value of frozen assets	2.95 billion EUR	3.05 billion EUR	2.84 billion EUR	4.62 billion EUR	4.92 billion EUR	4.44 billion EUR

6.3.1.5. Monitoring Committee

The Ministry of Finance chairs the Monitoring Committee on Financial Sanctions ("Monitoring Committee"), established in 2010[481]. The current legal reference for the Monitoring Committee is the Law of 20 July 2022. As a result of the entry into force of the Law of 20 July 2022, the AED became a standing member of the Monitoring Committee. The Committee holds regular meetings (on average 7-8 meetings per year – see table below) where its members discuss matters related to financial sanctions without limitation to any specific sanctions regime(s).

Table 23: Number of Monitoring Committee meetings held, 2017-2023[482]

Year	2017	2018	2019	2020	2021	2022	2023
Number of meetings	7	9	7	6	10	8	5

The Monitoring Committee brings together all authorities directly involved in matters of international financial sanctions. It deals with matters of legislative and regulatory updates, approval of best practices, identification of emerging risks and other trends as well as sharing of learning amongst competent authorities for further dissemination amongst supervised professionals. It does not, however, deal with individual cases of sanctions files under analysis by the Ministry of Finance.

480 Data provided by MoF for the purpose of this risk assessment. Reporting has been unified in EUR from 2022 onwards.
481 See the Grand-Ducal Regulation of 29 October 2010 (link) amended by the Grand-Ducal Regulation of 3 August 2011 (link).
482 All stakeholders may not have participated in all meetings.

In addition to the Ministry of Finance as chair, the Committee is composed of representatives of:

- Ministry of Justice
- Ministry of Foreign and European Affairs, Defence, Development Cooperation and Foreign Trade
- CSSF
- CAA
- CRF
- AED

The Monitoring Committee can furthermore invite to its meetings representatives of other public, judicial or administrative authorities, external experts, as well as representatives of the natural or legal persons having to apply the prohibitions and restrictive measures.

6.3.1.6. National/international cooperation

Considering the interconnected character of the financial sanctions with other sanctions regimes, the Ministry of Finance cooperates closely with the Ministries, authorities and SRBs involved in the implementation thereof. As such, the Ministry of Finance is a member of the export control working group (see subsequent section on OCEIT)**,** chaired by the representative of OCEIT. The participation of the Ministry of Finance in this working group is particularly important in the context of PF, considering the interconnection between the commercial transaction activating the export control mechanism and the subsequent/underlying financial transaction. The Ministry of Finance also cooperates with the CRF, on basis of a Memorandum of Understanding, and exchanges information with other national and foreign authorities as required for the implementation of TFS.

At European level, together with the Ministry of Foreign Affairs (which remains in charge of the overall coordination of sanctions/restrictive measures), the Ministry of Finance participates in the works of the Working Party of Foreign Relations Counsellors (RELEX/Sanctions Formation).[483] The Sanctions Formation was created in 2004 within the Working Party. Its main task is to share best practices and it also revises and implements common guidelines in order to ensure the effective and uniform implementation of EU sanctions regimes. The Ministry of Finance participates as well in the Commission Experts Group on restrictive measures and extraterritoriality.

At an international level, the Ministry of Finance also participates to FATF and the Counter ISIS Finance Group as part of the Global Coalition against Daesh.[484]

When it comes to specific sanctions files, the Ministry of Finance may contact the European Commission in order to obtain the Commission's view on the file under review. This occurs ad hoc and depends on each file (for example, when there are horizontal issues to be considered during the review of an authorisation requests that may affect the implementation of TFS at EU level).

In each case, this is done without disclosing the details of the file in question (names of operators, amounts involved or other information that could reveal the identity of the operator). The request is therefore formulated in general terms, with the Ministry of Finance asking for an opinion from the Commission (this may be informal or formalised later if the requesting country so wishes). For example, in 2021, the Ministry

[483] Section on the RELEX Working Group on the website of the European Council, accessed July 2025 (link)
[484] Website of the Global Coalition against Daesh, accessed July 2025 (link)

of Finance requested the opinion of the Commission in one case regarding DPRK and in another case regarding Syria.

6.3.2. Ministry of Foreign and European Affairs, Defence, Development Cooperation and Foreign Trade

Stakeholder	Key responsibilities related to TFS for PF and TF
Ministries	
Ministry of Foreign Affairs	• Competent for "coordination with regard to the implementation of international sanctions"[485] • "The Minister of Foreign and European Affairs, Defence, Development Cooperation and Foreign Trade is designated as the competent authority to communicate to the United Nations Sanctions Committees the natural and legal persons, entities and groups to which the restrictive measures in financial matters apply, as well as all information relating thereto, for the purpose of their inclusion on the United Nations Consolidated List"[486]

The Ministry of Foreign and European Affairs, Defence, Development Cooperation and Foreign Trade (Ministry of Foreign Affairs or MoFA), and more specifically its Directorate of European Affairs and International Economic Relations, is responsible for the general coordination of restrictive economic and financial measures decided by the United Nations and the European Union. As set out in the Law of 19 December 2020, the Minister of Foreign Affairs is also the competent authority for communicating with the UN Sanctions Committee.

In practice, this means that the Ministry of Foreign Affairs coordinates relations with international fora. At an international level, the Ministry of Foreign Affairs follows the work of relevant UN committees with regard to TFS for PF and TF. The Mission of Luxembourg to the UN in New York acts as intermediary between the Ministry of Foreign Affairs and all UN committees (including the UN Sanctions Committee established pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning the Islamic State of Iraq and the Levant (Daesh), Al-Qaida and associated individuals, groups, undertakings and entities, the UN Sanctions Committee established pursuant to resolution 1988 (2011), the UN Sanctions Committee established pursuant to resolution 1373 (2001) against terrorism and the UN Sanctions Committee established pursuant to resolution 1540 (2004)) passing on key information (where required), regular updates to the sanctions lists and receiving inputs/transmissions from the Ministry of Foreign Affairs. For example, in the past years, a question was asked to several countries (including Luxembourg) in relation to resolution 1970 (2011) imposing an arms embargo, a travel ban and an asset freeze in connection with the situation in Libya, to understand how member states with Libya-related frozen funds treated the payment of interest. Over the past years, the Ministry of Finance shared with the Ministry of Foreign Affairs, which subsequently submitted them through the Mission in New York, several exemption requests to the Security Council Committee established pursuant to resolution 1970 (2011) in relation to Libya regarding the payment of maintenance fees on frozen funds. More generally, the Ministry of Foreign Affairs follows the (more political)

[485] Grand-Ducal decree of 28 May 2019 establishing the ministries (link)

[486] Article 7, Law of 19 December 2020 (link)

developments related to sanctions in the UNSC as well as the discussions relative to the safeguarding of humanitarian space in countries under international sanctions.

At EU level, the Ministry of Foreign Affairs (via its representatives at the Permanent Representation of Luxembourg to the European Union (PREU)) participates in both RELEX[487] (which is generally held twice a week) and COMET[488] (which meets approximately 2-3 times per quarter, in a classified format). The Ministry of Foreign Affairs also participates in RELEX/Sanctions formation, which meets 2-3 times per semester.

The Ministry of Foreign Affairs intervenes in RELEX/COMET meetings, and in the past has transmitted information received from Luxembourg national authorities. The information served as basis for a designation proposal at EU level (and resulted in a designation).

Outside of formal UN/EU fora, where international requests are received (regardless of channel, e.g. these may be received by the Ministry of Foreign Affairs or by the Ministry of Finance), answers are collected in partnership with relevant agencies (e.g. impacted supervisors) and coordinated by the Ministry which received the initial request. Once collected, the answer is given by the most appropriate agency (often, not always, the agency which received the initial request). This approach and ministerial coordination help reduce the workload on operators.

At national level, the Ministry of Foreign Affairs participates in the Monitoring Committee and in the sub-group created on 21 September 2022 working on national designations. The Ministry may also receive communications directly from operators (e.g. regarding the conduct of business in countries which are sensitive from a PF/TF perspective, in order to better understand the relevant sanctions regimes, etc.). If it would be more appropriate to discuss the matter directly with the MoF, correspondence will be passed on to the latter. The Ministry of Foreign Affairs furthermore constantly (usually on a weekly basis) exchanges with the MoF on sanctions-related matters.

The Ministry of Foreign Affairs and the CRF signed on 1 April 2022 a Memorandum of Understanding which covers the exchange of information in areas of converging interest – for instance if the facts that gave rise to economic and financial restrictive measures are also likely to give rise to a suspicion of money laundering, where a DNGO is abused or likely to be abused to commit or facilitate money laundering or where a suspicion of money laundering arises in relation to a person carrying out an activity prohibited or subject to authorization under the Law of the 27 June 2018 on export controls. The Memorandum of Understanding therefore enables the consultation, cooperation and exchange of information between these two entities in the field of AML/CFT.

Alongside its competence related to international restrictive measures, the Ministry of Foreign Affairs also plays additional roles that contribute more indirectly to Luxembourg's overall counter-TF/counter-PF framework. Export licenses that enable the export of dual-use and military items to third countries are co-signed by the minister of Foreign Affairs and the minister of Economy.[489]

Moreover, the Ministry of Foreign Affairs plays a role in market entry for certain particular legal persons, specifically NPOs engaging in development and humanitarian projects abroad and accredited as such by the Ministry of Foreign Affairs. NPOs such as ASBLs and *fondations*, which have as their purpose in particular development cooperation, may indeed be accredited as non-governmental organisations for development

[487] Working party of Foreign Relations Counsellors, in charge of legal, financial and institutional issues of the Common Foreign and Security Policy (CFSP), including sanctions.

[488] Working Party on restrictive measures to combat terrorism (COMET).

[489] Following the change of government after the October 2023 general elections in Luxembourg (with the new government being sworn in on 17 November 2023), responsibility for export licences was transferred to the Ministry of Foreign Affairs. As a result, export licences are currently examined by two directorates, with the Minister signing in a dual capacity (Foreign Affairs and External Trade).

(DNGO)[490]. The accreditation is granted by the Ministry of Foreign Affairs upon request from the organisation justifying its technical and financial capacities, as well as its skills and experience in implementing development cooperation programmes or projects that benefit populations in developing countries. As of December 2023, 91 NPOs were accredited as DNGO[491].

6.3.3. Ministry of Justice

Stakeholder	Key responsibilities related to TFS for PF and TF
Ministries	
Ministry of Justice	• Has no specific competencies related to TFS but is competent for matters regarding FATF[492] • Has responsibilities related to CFT

The Ministry of Justice does not have competencies related to the implementation of TFS. That said, its competencies – as set out in the Règlement interne du Gouvernement[493] – include matters regarding FATF. It therefore holds some responsibilities which are related to TFS, such as:

- Chairing the national prevention committee on AML/CFT, which includes monitoring effectiveness for Immediate Outcomes 10 and 11 and Recommendations 6 and 7
- Coordinating FATF submissions and visits, which includes an assessment of Luxembourg's framework for TFS
- Participating on behalf of Luxembourg in relevant international fora for FATF-related matters, which includes tangentially monitoring progress on the elements of TFS that overlap with FATF mandate
- Attending Monitoring Committee meetings
- Performing market entry checks for particular legal persons, namely fondations and ASBLs with public utility status, which have similar obligations as fondations[494]

[490] Article 7 of the law of 6 January 1996 on cooperation to development and humanitarian action, as modified and as completed by the Grand-Ducal Regulation of 7 August 2012
[491] Website of the Ministry of Foreign Affairs (link)
[492] Règlement interne du Gouvernement (link)
[493] Règlement interne du Gouvernement (link)
[494] Further details may be found in Luxembourg, *ML/TF Vertical Risk Assessment Legal Persons and Legal Arrangements* (section 5.4.4.2.), 2022 (link)

6.4. Supervisors and SRBs

6.4.1. CSSF

Stakeholder	Key responsibilities related to TFS for PF and TF
Other public authorities	
Commission de Surveillance du Secteur Financier (CSSF)	• Responsible for "prudential, AML/CFT including TFS supervision of professionals of the financial sector falling under the scope of its competences". On the basis of Article 33 of CSSF Regulation no. 12-02, these persons are required i.a. to keep the CSSF informed when natural and legal persons, entities or groups involved in a transaction or business relationship subject to prohibitions or restrictive measures in financial matters are identified[495] • "Has the same powers as those conferred by Articles 8-2, 8-4, 8-5, 8-6, 8-7 and 8-9 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended"[496]

The CSSF is responsible for the prudential and AML/CFT supervision of professionals of the financial sector, which includes sanctions implementation matters (for PF, TF and other sanctions regimes)[497]. Professionals' obligations in relation to Targeted Financial Sanctions (TFS) are set out in the Law of 19 December 2020[498]. They are also specified in the CSSF Regulation No 12-02 (articles 33, 38, 39 and 39 (1a)), unless otherwise defined. These obligations concern the implementation of TFS and practical details (e.g. what to screen, how frequently to screen).

The CSSF, as part of its AML/CFT supervision, monitors the extent to which supervised professionals have processes and controls in place to meet their obligations in relation to TFS, via market entry controls, ongoing supervisory activities (on-site and off-site) and regular interaction and guidance with/to the supervised professionals. The supervisory approach deployed by CSSF across its supervised entities is largely the same for any sanctions regime; however, for the purposes of this risk assessment, the mitigating factors described focus on PF and TF-TFS regimes in particular. Accordingly, CSSF is kept informed by professionals when persons, entities or groups are identified as involved in a transaction or business relationship subject to prohibitions or restrictive measures in financial matters, irrespective of these being regarding the fight against PF and TF or other regimes[499].

The CSSF operates a federated or decentralised organisational model, with off-site and on-site specialist teams (as captured in the table below) covering each supervised sector, alongside a central team (LCF[500]) which acts as a coordinating mechanism. Approaches for supervising TFS implementation are broadly consistent across supervised sectors and the responsible supervisory departments.

[495] Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals*, 2021 (link)

[496] Article 6(5) of Law of 19 December 2020 (link)

[497] For VASP, PI/EMI agents/distributors, and registered AIFMs, the CSSF only carries out AML/CFT and TFS supervision, but no prudential supervision.

[498] Law of 19 December 2020 (link)

[499] As per CSSF Regulation No 12-02, Article 33 (link)

[500] "LCF" stands for "*Lutte contre la Criminalité Financière*" (formerly known as "JUR-CC").

Table 24: CSSF supervisory departments[501]

Department	Relevant supervisory scope[502]	Sub-sector
Banques (B)	Banks	• Retail & business banks (including entities operating online) • Wholesale, corporate & investment banks • Private banking • Custodians and sub-custodians (including CSDs)
Entreprises d'investissement (EI)	Investment sector (Wealth managers[503])	• Investment firms authorized to carry out the services of investment advice and portfolio management[504]
Organismes de Placement Collectif (OPC)	Investment sector	• Collective investments[505]
Innovation, paiements, infrastructures des marchés et gouvernance (IPIG)	Money or Value Transfer Services (MVTS)	• Payment institutions (PIs) • E-money institutions (EMIs) • Agents and e-money distributors acting on behalf of PIs/EMIs established in another EU Member State
Innovation, paiements, infrastructures des marchés et gouvernance (IPIG)	Virtual Asset Service Providers (VASP)	• Virtual Asset Service Providers[506]
Professionnels du Secteur Financier spécialisés (PSF SP)	Specialised PFSs	• Specialised PFSs providing corporate services[507]

It is important to note that requirements for supervised professionals, and the supervisory controls described in the sub-sections below, relate to the implementation of TFS specifically. For TF more broadly, there are additional obligations and controls in place, included in the broader AML/CFT framework by CSSF and supervised professionals, which are described in the 2020 NRA and in the 2025 NRA, as well as more specifically in Luxembourg's TF VRA. The obligations for PF and TF sanctions implementation are derived

[501] Where sectors/sub-sectors were not subject to a deep-dive analysis for this assessment (e.g. 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, 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, Regulated securitization vehicles, CSSF-supervised pension funds, Professional depositaries, Market operators, Support PFSs & other Specialised PFSs), they have not been included in this table; moreover, transfer agents are not explicitly referenced in this assessment as they are not identified as high-risk by FATF, but should be included in aggregated sectoral data, where relevant.
[502] Refers to shortlisted sectors only.
[503] Formerly known as "Wealth and asset managers" (*gérants de fortune*).
[504] Other types of entity supervised by EI are excluded from this table as they were not subject to a deep-dive analysis for this risk assessment.
[505] Investment funds and managers supervised for AML/CFT purposes by the CSSF. Other types of entities supervised by the CSSF are excluded from this table as they were not subject to a deep-dive analysis for this assessment.
[506] Excluding Banks offering Virtual Asset Services, which are supervised by Banques (B).
[507] Other types of Specialised PFS supervised by the CSSF are excluded from this table as they were not subject to a deep-dive analysis for this assessment.

from Luxembourg's legal and regulatory framework which today completely includes UN and EU sanctions regimes, as well as national sanctions regimes, if/when applied. Having said that, a number of supervisory measures cited and referred to in the present VRA on PF and TF TFS have their origin in supervision of other TFS regimes, notably the financial restrictive measures decided in the context of the war against Ukraine. Indeed, a number of awareness-raising activities of the CSSF have a general scope and are valid for any kind of TFS. They will therefore be taken into account in this assessment.

Whilst the MoF is competent with respect to TFS, the CSSF is responsible to monitor that supervised professionals implement procedures and controls with respect to TFS.

The CSSF is also a member of the Monitoring Committee.

6.4.1.1. Market entry controls

The CSSF will not grant an authorisation to any professional linked to a person/entity subject to TFS.

The CSSF's market entry controls (for licencing, registration and notification) generally ensure that the natural and legal persons subject to TFS are prevented from holding or being the beneficial owner of a significant or controlling interest or holding a senior management/key function in relevant financial institutions, including DNFBPs or VASPs under its remit.

The main mechanism during the formal licensing process to mitigate TFS risks relates to "fit and proper" assessments conducted on relevant persons[508]. For these assessments, the CSSF conducts a series of checks which includes central screening against national and international sanctions lists (including those related to TF and PF). It is worthwhile to note that for prudential licensing requirements the identification of beneficial owners holding 10% is required.[509] For Banking entities, the CSSF adopts policies and guidelines from the ECB and the EBA.

The CSSF also conducts assessments on certain individuals associated with professionals not required to obtain a licence, but which are required to register (e.g. executive managers and beneficial owners of VASPs[510]).

Moreover, the CSSF ensures that each applicant (i.e. future obliged entity) has adequate AML/CFT related policies and procedures in place.

These market entry controls are repeated during the life cycle of the professional each time changes occur, for example where a significant shareholder or manager changes.

Pursuant to these market entry checks, there has not been a recent case where the applicant was subject to TFS for PF or TF.

6.4.1.2. Understanding of PF/TF TFS risks

The CSSF promotes understanding among supervised professionals of PF and TF TFS and of the risks associated with the breach, non-implementation or evasion of TFS, namely by:

---

508 Including: members of the management body; beneficial owners; and (in)direct shareholders holding 10% or more of the entity's capital or voting rights or exercising significant influence on its management (and/or having effective control over the decisions of the entity).

509 (In)direct shareholders holding 10% or more of the entity's capital or voting rights or exercising significant influence on its management, stressing that a beneficial owner is not only determined with respect to a threshold (see article 1(7) of the 2004 AML/CFT Law).

510 As set out in Art. 7-1(3) and (3a) of the 2004 AML/CFT Law.

- **Regularly publishing related guidance/information**: This includes specific **circulars CSSF** on high-risk countries such as DPRK and Iran (e.g. Circulars CSSF 10/458, 07/327 and 06/247); [511] **press releases** on TFS (e.g. Press Release 11/08);[512] **Circular letters** (e.g. Circular letter of 1st of March 2022, related to EU restrictive measures in response to the situation in Ukraine)[513], "**Communiqués**" (e.g. Communiqué of 8 April 2022 on restrictive measures of the EU in response to the current situation in Ukraine and anti-money laundering and counter terrorist measures[514]; Communiqué of 25 October 2023 relating to the terrorist organisations of Hamas and the Palestinian Islamic Jihad; Communiqué concerning non-profit organisations and the fight against terrorism financing of 30 May 2024[515]), **FAQs** (e.g. FAQs on "International Financial Sanctions"[516]or an FAQ relating to the use of the guidelines of the Ministry of Finance)[517] and **guidance** in its annual activity report[518]. Moreover, the CSSF has also published in its **Newsletter** information relating to the FATF Guidance on Proliferation Financing Risk Assessment and Mitigation[519], on the December 2020 joint paper of FATF and Egmont Group of Financial Intelligence Units on trade-based ML, on the Law of 19 December 2020 among others, and provided notably awareness, through a "Communiqué", of the redesign of the website of the MoF regarding international financial sanctions[520]. The CSSF also published in October 2023 a link on its website to the Annual Progress Report on the Implementation of the European Union Strategy against the Proliferation of Weapons of Mass Destruction[521].
- **Regularly publishing the latest FATF statements** on high-risk jurisdictions and jurisdictions under increased monitoring. In its publications (in particular via the updated annex to Circular CSSF 22/822), the CSSF i.a. raises awareness regarding strategic deficiencies of the AML/CFT and PF regimes related to jurisdictions that are subject to a FATF call on its members to implement both TFS and countermeasures against these countries. For example, Circular CSSF 21/786 notably relates to Iran and DPRK, and its appendix requests professionals to inform the CSSF of any correspondent banking relationships with credit institutions from these two jurisdictions[522]. The CSSF also shares or even summarises related FATF publications in its monthly newsletter[523].
- **Promoting understanding through ongoing supervisory activities and by providing feedback on TFS related deficiencies found through supervisory activity (off-site and on-site)**: For example, awareness-raising and guidance is provided during on-site AML/CFT inspections in case of deficiencies found by the CSSF teams. In 2020, for example, the Banking Department sent a letter to all relevant professionals (as they are the most exposed) to clarify expectations in relation to the annual Financial Crime Survey and the questions on TFS implementation (reference is made to the case study below titled "Awareness-raising with regard to freezing of funds or other assets without delay after designation on sanction lists"). Moreover, for example in 2018, the CSSF published via its annual activity report very detailed findings

[511] Various circulars from CSSF: Circular CSSF 10/458, 2010 (link); Circular CSSF 07/327, 2007 (link); Circular CSSF 06/247, 2006 (link)
[512] CSSF Press Release 11/08, 2011 (link)
[513] CSSF circular on restrictive measures of the EU in response to the current situation in Ukraine, 2022 (link)
[514] CSSF Communiqué on restrictive measures of the EU in response to the current situation in Ukraine and anti-money laundering and counter terrorist financing measures, 2022 (link)
[515] CSSF Communiqué concerning non-profit organisations and the fight against terrorism financing, 2024 (link)
[516] CSSF FAQ regarding International Financial Sanctions, 2022 (link)
[517] CSSF FAQ relating to the use of the good conduct guide Ministry of Finance, 2016 (updated in 2021) (link)
[518] CSSF, *Annual Report 2014*, 2015 (link)
[519] CSSF Newsletter 247 (page 8), 2021 (link)
[520] CSSF Communiqué on *redesign of the website of the Ministry of* Finance, 2021 (link)
[521] CSSF, *Annual Progress Report on the Implementation of the European Union Strategy against the Proliferation of Weapons of Mass Destruction (2022)*, 2023 (link)
[522] Circular CSSF 22/822 as updated (link) is the latest circular on this subject.
[523] Reference is made for instance to Newsletter CSSF No. 295, 2025 (link).

and specified regulatory expectations[524]. The CSSF's 2020 annual activity report also included a specific focus on the adoption of the Law of 19 December 2020. In the context of the TFS against Russia, multiple awareness raising activities have been implemented by the CSSF. Supervisory expectations with respect to TFS controls are also discussed for example within CSSF AML/CFT Expert Working Groups with representatives i.a. of the private sector or when adopting new regulations, as for instance CSSF Regulation 20-05.

- **Continually organising and participating in industry events** where agenda items include TFS. This includes external events such as ALCO-ALJB conferences[525] and CSSF-organized conferences[526], CSSF-co-organized conferences (e.g. with the ABBL[527] or the ALCO) and CSSF Expert Working Groups[528].

Table 25: Information maintained on the CSSF's website related to international financial sanctions[529]

Relevant section	Description
Laws, regulations and directives	Provides links to relevant laws, including the Law of 19 December 2020 and (although now repealed with regards to the TFS part) the law of 27 October 2010
UN decisions and ministerial regulations with respect to the fight against terrorism financing	Links to UN resolutions and associated designations that are relevant for TF
Texts adopted by the EU with respect to the fight against terrorism financing	Links to EU Council regulations that are relevant for TF
Texts related to the fight against the financing of proliferation of weapons of mass destruction	Links to EU regulations, FATF guidance and relevant publications for PF
Other prohibitions and restrictive financial measures in relation to specific countries	Links to EU Council regulations for sanctions regimes involving restrictive financial measures, including those in-scope for this report
Documentation	Several documents, including reference texts, forms, guidance (e.g. FATF reports), publications Links to the MoF's website

The CSSF also works bilaterally with the MoF to identify good and bad practices in relation to compliance with obligations regarding TFS and collaborates to promote areas for improvement. The MoF keeps the CSSF informed of and discusses with the CSSF the information submitted by professionals under the CSSF's remit for the purpose of the CSSF's supervisory tasks.

---

[524] Reference is made for instance to CSSF 2018 Annual Report, p. 152: "*several problems were encountered in relation to name matching controls against the official lists of international financial sanctions, including, among others, unsatisfactory control frequency, given that these controls must be carried out at least when these lists are published, insufficient materialization of the results of the analyses carried out and incomplete controls (failure to ensure the exhaustiveness of the data recorded in the system on which the controls are based)*".

[525] On 15 June 2021 took place an ALCO-ALJB Conference on international financial sanctions that included a special focus on the role and powers of supervisory authorities.

[526] The CSSF 2022 AML/CFT Conference dedicated to Specialised PFS included a focus on TFS and PF (link).

[527] In October 2019, the annual ABBL-CSSF conference included a session presented by the MoF on the topic of "International financial sanctions: Legal framework and obligations of the operators".

[528] In April 2021, the Expert Working Group on ML/FT risks in private banking, gathering the CSSF, the CRF, the ABBL and representatives from banks, included a dedicated presentation and discussion on TFS and PF-related risks.

[529] Section of the CSSF website on international financial sanctions, accessed July 2025 (link)

6.4.1.3. Prevention/private sector controls

Professionals have access to a range of methods to ensure they understand and implement their AML/CFT obligations, as well as those related to PF and TF-TFS.

- **Reviewing guidance** and regulations issued by national and international authorities: for example, the MoF's guidelines on TFS[530], CSSF Regulation No 12-02 (specifically articles 33, 38(2)17, and 39(1) and (1a) specifying professionals' obligations regarding TFS[531]), CSSF guidance published in annual activity reports of for example 2014, 2018 and 2020 specifying supervisory expectations, and FATF guidance on counter-PF[532]. See above for an outline of the awareness-raising and information measures in place.
- **Interacting with the CSSF** as part of its supervisory activities, such as to understand areas where client screening processes and tools can be further enhanced. For example, as a result of interaction between a supervised professional and the CSSF, the tool used by the supervised professional and provided by a Luxembourg provider could be improved (by requiring the provider to increase the frequency of updates to the tool), thereby having a positive impact on all supervised professionals having used/using this tool.
- **Documenting obligations** and the processes required to meet them in policies and procedures: for example, those related to TFS screening (as required by article 38(2)17 of CSSF Regulation No 12-02)
- **Implementing training programs** (that can cover AML/CFT and TFS topics: including specific references to PF in some cases) to promote understanding of obligations related to TFS among staff (for example participating in the ABBL/CSSF conference of October 2019 whereby the MoF provided guidance on TFS to an audience in excess of 250 professionals).
- **Interacting with industry associations (e.g. ABBL, ALJB, ALFI and ALCO)** and other bodies to strengthen understanding of both obligations relating to TFS and potential exposures to PF/TF. For example, the subject of investment-related screening has been extensively discussed by supervised professionals and their representative bodies in the context of the AML/CFT OPC Expert Working Group put in place by the CSSF, which led i.a. to amendments of article 39 (1a) of CSSF Regulation No 12-02 (previously foreseen in Circular CSSF 18/698) and updates currently undertaken to industry guidelines by ALFI. Moreover, as already referenced, the CSSF participates in training activities, such as the training organised between

[530] Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals*, 2024

[531] Article 33: "(*1) Ongoing due diligence referred to in point (d) of the first subparagraph of Article 3(2) of the Law shall include at least the obligation to identify without delay:*

> *- pursuant to Article 8(2) of the Grand-Ducal Regulation and in accordance with the Law implementing restrictive measures in financial matters, the States, persons, entities or groups involved in a transaction or business relationship subject to restrictive measures in financial matters in the context of the fight against terrorist financing, including, notably, those implemented in Luxembourg via EU regulations directly applicable in national law or through the adoption, among others, of ministerial regulations; and*
>
> *- the States, persons, entities or groups involved in a transaction or business relationship subject to restrictive measures in financial matters, including, notably, those implemented in Luxembourg via EU regulations directly applicable in national law or, where appropriate, through the adoption of regulatory texts implementing them at national level.*

(2) Where persons, entities or groups referred to in this article are identified, and without prejudice to the obligations laid down in Article 5 of the Law and Article 8 of the Grand-Ducal Regulation, the professional shall apply, without delay the required restrictive measures and inform the authorities competent for financial sanctions.
A copy of this communication shall be sent to the CSSF at the same time."
(3) Following the adoption or update of the official lists as referred to in paragraph 1, the professional shall ensure that the internal system used for this control or made available by an external service provider which it uses for the purposes of this control is adapted without delay in order to be able to comply with the obligations under paragraphs 1 and 2 of this article."
Article 39 provides for the processes to be put in place by professionals and specify also in its paragraph (1a) that, "*for the purposes of Article 33 of this regulation, the professional also has the obligation to identify the States, persons, entities and groups subject to restrictive measures in financial matters with respect to the assets it manages and to ensure that the funds will not be made available to these States, persons, entities or groups*".

[532] For example, FATF, *Guidance on Counter Proliferation Financing*, 2018 (link) and FATF, *Guidance on Proliferation Financing Risk Assessment & Mitigation*, 2021 (link)

ALCO and CSSF in June 2021 on the topic of international financial sanctions and the role of the competent authorities and the sanctioning powers of the CSSF, as well as in May 2023 on good practices in TFS-related matters together with ALCO, the MoF and the CRF.

To ensure their obligations are fulfilled, supervised professionals must implement several processes, in line with i.a. articles 33, 38 and 39 of CSSF Regulation No 12-02:

- **Screening potential customers/BOs/proxies** against national and international (EU/UN) sanctions lists (including TF and PF-TFS) before establishing a new business relationship;
- **Screening existing customers/BOs/proxies** against new/updated lists (without delay) when they are published, as well as screening clients/BOs/proxies against existing lists when they periodically re-conduct due diligence measures;
- **Screening transactions** throughout the course of the business relationship to identify those that may be related to legal or natural persons subject to TFS (screening usually takes place before carrying out wire transfers by debt of customer account or before crediting incoming funds to customer accounts);
- **Taking into account the higher geographical risk associated with the relationship**, i.e. customer/BO/proxy from a country associated with PF (Iran and DPRK) or with TF (e.g. Afghanistan), **or the transaction.** The CSSF has issued specific guidance on higher risk jurisdictions, such as Circular CSSF 22/822, which relates to high-risk jurisdictions in terms of ML/TF, but also PF;
- **Informing the CSSF when entering into correspondent relationships with financial institutions from Iran or from DPRK, which has never occurred.**

Supervised professionals have several mechanisms for ensuring such screening is against the most up-to-date lists. Supervised professionals can refer to automated screening tools from specialist external providers, as well as the national and international (EU/UN) sanctions lists (whose consolidated versions are available on the CSSF and MoF websites), sanction-specific mailings from the CSSF and information from websites of other relevant national and international bodies such as the UN, FATF and EU.

Should supervised professionals identify a transaction or business relationship involving individuals, entities, groups or States subject to TFS, they shall without delay freeze the funds and economic resources belonging to these individuals, entities, groups or States, and promptly report to the MoF with the CSSF in copy. Correspondingly, following the de-listing of formerly designated individuals, entities, groups or States [subsequent to an EU regulation or an amending UN resolution] noticed by supervised professionals as part of their ongoing due diligence obligations, they should also take action to de-freeze funds and assets.

Notwithstanding this, the CSSF has identified instances where supervised professionals' monitoring processes for TFS required strengthening, or where reporting was not carried out "without delay".

Alongside screening, there are additional checks to ensure appropriate due diligence is possible. For example, to mitigate potential risks that could arise due to remote client on-boarding, more stringent pre-authorisation requirements apply in these cases. For non-face-to-face client onboarding, additional measures must be applied in accordance with article 27 of the CSSF Regulation No 12-02 as amended. An additional FAQ clarifies supervisory expectations when resorting to non-face-to-face client onboarding[533].

[533] CSSF, *FAQ on AML/CTF and IT requirements for specific customer onboarding/KYC methods for the identification/verification through video chat,* 2018 (link)

6.4.1.4. Supervision and enforcement

The CSSF applies a risk-based approach to AML/CFT supervision, in line with guidelines and recommendations of international and European standard setters. This includes matters relating to TFS implementation supervision, notwithstanding the fact that obligations for sanctions implementation apply to all supervised professionals. There are broadly two mechanisms for the CSSF to monitor the effectiveness of professionals' processes and controls to ensure that they meet their obligations in relation to PF- and TF-TFS: (1) on-site and (2) off-site activities (see below).

The CSSF cooperates with international/European authorities or bodies and with national authorities to stay up-to-date with the latest trends and typologies with respect to TFS.

Specific country lists were drawn up and developed internally and are available to all CSSF agents to be used in the context of their supervision. These lists identify countries with risks regarding TF, financial restrictive measures or potential circumventions of financial restrictive measures.

6.4.1.4.1. On-site inspections

Controls on sanctions screening are included as part of all full-scope on-site inspections for AML/CFT, with no differentiation per supervised sector. They can also be part of partial-scope inspections, depending on the topic. In 2022 and 2023, thematic on-site inspections with regard to TFS have taken place that included also the subject of sanction evasion. These on-site missions allowed observing that the professionals actively cooperated with the authorities to ensure the respect of TFS. No case of non-compliance with the restrictive measures was detected. Regarding non-proliferation financing, the CSSF drew the attention of the professionals on the compliance with sectoral sanctions which require an in-depth review of the transactions originating from or addressed to a country subject to targeted financial sanctions. Another thematic onsite inspection launched in 2022 and conducted in 2023 was regarding trade finance activity by professionals that could be of relevance in particular for proliferation financing risks and TFS. Following this on-site inspection, the CSSF requested for example a better formalization of the analysis performed, especially on the trading routes and on the nature of the traded goods.

During these on-site inspections, the CSSF examines the adequacy, completeness and effectiveness of controls in place in relation to TFS (in general).

The most common findings regarding TFS implementation from on-site reviews relate to professionals having deficiencies in their internal procedures for screening, not updating the database or tool to be used for screening, not screening parts of the database, not screening with sufficient frequency, or IT issues relating to sanctions tool interface or integration with internal systems. Findings on the quality of investigations also occur, but more often about adequate formalization (i.e. ensuring appropriate documentation to determine true/false alerts from sanctions screening software). Still, it is noted that the general maturity of investigations over sanctions screening alerts at supervised professionals for TFS is lower than for ML, in particular for PF and for smaller professionals that may not have a fully automated investigations process. Queries and exchanges on open investigation cases are often made directly with the MoF (with the CSSF in copy) and can be complex and long.

Where compliance failures are identified, the CSSF follows up with the professional with measures depending on the severity of the shortcoming. However, the CSSF has observed a general trend for professionals to perform the name-screening control more and more often on a daily basis, especially within large actors.

Case study: Inadequate frequency of the name-screening controls, leading to an administrative fine

- In September 2019, the CSSF carried out an on-site inspection on the AML/CFT framework of a bank. Several deficiencies were identified, in particular regarding the name-screening controls of the bank aiming at detecting persons, entities or groups involved in a transaction or business relationship subject to restrictive measures in financial matters (i.e. TFS).
- As per the bank's procedures, these controls were supposed to be performed twice a month. Hence, there was no control performed immediately when a new sanction list was published. Moreover, this control was manually triggered and the CSSF noted that due to human errors the theoretical frequency "twice a month" was not respected.
- This inadequate frequency had no direct impact, i.e. no late filing was made to the authorities. However, the CSSF considered it was a severe weakness and, also considering the other deficiencies observed (related to the general AML/CFT framework but not specifically to FT), the CSSF decided to impose a pecuniary sanction and to publish the sanction (in a nominative manner).
- As a remediation action, the bank put in place a daily automated name-screening control.

Case study: Inadequate frequency of the update of the TFS lists based on which a bank performed its name-screening controls, leading to an administrative fine

- In 2020, the CSSF carried out an on-site inspection on the AML/CFT framework of a bank, where severe deficiencies were observed regarding the name-screening controls on the client database. The CSSF especially noted that, despite the fact that the frequency of these controls seemed adequate (the controls were performed on a daily basis), the TFS lists on which the bank based its controls were updated irregularly and not immediately once a new sanction list was published. The lists had even not been updated during a one-year period.
- Also, considering the other deficiencies (related to the general AML/CFT framework but not specifically to FT), the CSSF decided to impose a pecuniary sanction and to publish the sanction (in a nominative manner).
- After this on-site inspection, the bank put in place a daily control to ensure that the TFS lists embedded in its name-screening system were up to date.

Case study: Severe deficiencies relating to the general name screening controls performed by an electronic money institution, leading to an administrative fine

- In 2021, the CSSF carried out an on-site inspection on the AML/CFT framework of an electronic money institution. Several deficiencies were identified, in particular regarding the name screening controls of the electronic money institution aiming at detecting persons, entities or groups involved in a transaction or business relationship subject to restrictive measures in financial matters (i.e. TFS). In this respect, the CSSF highlighted that a significant number of active and blocked clients were not subject to the name screening controls performed by the electronic money institution on a daily basis.
- The finding related to the absence of name screening controls for certain client groups/involved parties was considered as a severe breach and triggered an enforcement (sanctioning) process.
- As a result of CSSF's actions, the electronic money institution confirmed that it had included all the missing clients in the database that is screened on a daily basis against financial sanctions lists. It resulted in a certain number of hits which were finally reported to the CRF. Out of those hits, some related to sanctions lists but neither related to United Nations Security Council resolutions, acts adopted by the European Union (resolutions and acts

directly applicable in Luxembourg) nor national regulations (Luxembourg) concerning prohibitions and/or restrictive measures in financial matters with respect to certain States, persons, entities or groups in the context of the fight against terrorist financing or with respect to other financial embargos.

- Even if this finding was not PF/TF-TFS specific (controls are not regime specific), the remediation made it possible to contribute to proper PF/TF-TFS screening.

6.4.1.4.2. Off-site activities

As part of its off-site supervisory activities, the CSSF reviews key reports (e.g. the statutory auditor report, the AML/CFT Compliance function report, the internal audit report and the internal control report) to monitor closely whether any deficiencies have been identified in relation to name matching and transaction screening (incl. against TF or PF-TFS lists). While the CSSF detected some instances of deficiencies in relation to the screening obligations, there were no hits identified related to TF or PF-TFS that should have been identified by the professionals. Professionals have reported to the MoF relevant cases and this confirms that adequate systems are in place to enable compliance with UN resolutions and EU regulations. All CSSF departments systematically follow up on identified deficiencies and require remediation actions by professionals.

Lastly, **off-site activities include the collection and processing of responses to the annual Financial Crime Survey per supervised sector which includes dedicated questions to TFS implementation** (references to which are made throughout this text). In 2021, these targeted questions for TFS implementation were further harmonized across CSSF sub-sectors.

Other cases of the CSSF's actions are shown below. To note that the CSSF's supervisory activity relates to TFS in general and is not PF/TF TFS specific and thus that any conclusions regarding the following cases must take this caveat into account.

Case study: Injunction letter sent after a follow-up of a deficiency relating to screening of TFS lists identified during an AML/CFT on-site inspection

- In 2018, as part of the ongoing supervision of a Specialised PFS, an issue relating to the incomplete database was identified by the on-site inspection team and an observation letter was sent to this Specialised PFS. Six months after the letter sent to the professional requiring remediation, the CSSF also found out that the Specialised PFS was in the process of migrating data to a new database and was screening two databases against TFS lists, but that none of the databases were complete. The Specialised PFS advised that another entity of the group was assisting with the input of the data and that the database would be completed within the same year.
- The CSSF sent an injunction letter to the Specialised PFS and gave one month to complete the information on the new database.

Case study: Awareness-raising with regard to freezing of funds or other assets without delay after designation on sanction lists

Following exchanges with the banking sector as part of the annual CSSF & ABBL Compliance Conference on AML/CFT, the Expert Working Group on ML/FT risks in private banking or bilateral meetings with Chief Compliance Officers, the CSSF realized that there was a need to clarify certain principles regarding the obligations of banks in relation to national and international financial sanction regimes.

On 3 February 2020, the CSSF sent an email to the attention of the Chief Compliance Officers of all banks to remind them on the requirements and expectations with regard to:

- The screening scope (Article 39 (2) of CSSF Regulation No 12-02) and the fact that the screening scope is not subject to any risk-based approach
- The screening timing (Article 39 (1) of CSSF Regulation No 12-02)
- The screening documentation (Article 39 (3) of CSSF Regulation No 12-02)
- The screening frequency (Article 33 of CSSF Regulation No 12-02 and FATF Recommendation 6 requiring to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any “listed” person or entity)
- The obligation to update screening tools without any delay with the names of newly designated or de-listed persons or entities after the publication of the measures by the CSSF and/or the MoF
- The alert handling (Article 33 (2) of CSSF Regulation No 12-02)
- How to stay informed on new financial sanctions

Moreover, banks which had not reported daily name screening and/or ad hoc update frequencies of screening tool lists in their responses to the annual Financial Crime Survey sent to the CSSF were contacted in order to request more information on the situation and, as the case may be, were requested by injunction letter to remediate the screening frequencies or list updates accordingly.

The CSSF’s awareness raising measure was also put on the agenda of the meeting of the Private Banking Expert Working Group dated 28 February 2020 and the clarifications provided in the CSSF’s email to the Compliance Officers dated 3 February 2020 were highly welcomed by the group members.

Based on the responses to the CSSF Financial Crime Survey received in 2020, the CSSF had identified a number of banks which did not report a daily name screening or list update frequency. After contacting these banks for further clarifications, the CSSF finally sent injunction letters to several banks, requesting to take remedial actions. All of these banks meanwhile confirmed having put in place either daily screening or ad hoc screening frequencies upon publication of new lists.

Following the request, some of the smaller banks, mainly those which performed semi-manual ad hoc screenings upon publication of new lists, also informed CSSF that they now decided to implement fully automated daily screening tools.

Case study: Example of follow-up measures taken by the CSSF with regard to Iran/DPRK/Myanmar

- This case concerns the follow-up by the CSSF on information regarding alleged wire transfers with the DPRK, cooperation with national authorities.
- The CSSF noted, from exchange of data with the BCL on financial flows in/out of Luxembourg, that a bank had reported wire transfers with the DPRK to BCL.
- The CSSF contacted the bank to request detailed information on the relevant transactions. The bank reported back to the CSSF that after internal investigation they found that these payments were originated in another country. The reference to the country code for DPRK (KP) quoted in the report sent to BCL appeared to have been generated due to a technology coding issue that was then resolved.
- There was a follow-up by the CSSF to ensure that relationships identified with Iran and Myanmar have been properly subject to EDD by the corresponding banks.

Case study: Correspondent banking relationships with Iran or DPRK

- This case concerns the use of Circular CSSF 22/822 and its quarterly updates on FATF statements regarding Iran and DPRK to collect updated information.

- In addition to information contained in the annual Financial Crime Survey collecting information on geographic risks (related to customers[534], transactions and volumes) and TFS compliance, the CSSF systematically requests information on correspondent banking relationships with Iran or DPRK via its quarterly circulars updating on the latest FATF statements on high-risk jurisdictions and jurisdictions under increased monitoring. The CSSF has not been informed about any correspondent banking relationship with entities from Iran or DPRK.

Case study: Follow-up measures taken by the CSSF regarding the processing time for hits generated by the name screening tool and/or transaction screening tool against restrictive measures and Targeted Financial Sanctions lists

Following the review of data included in the 2022 Financial Crime Survey of the CSSF, the CSSF realized that there was a need to clarify certain principles regarding the processing time of alerts related to the ongoing monitoring systems within banks in relation to national and international financial sanction regimes.

On 6 September 2023, CSSF sent a letter to a number of banks to remind them of the requirements and expectations with regard to screening controls that must be performed without delay after the publication of each new adoption or amendment of the national and/or EU, UN targeted financial sanctions lists, in line with the following legal and regulatory requirements:

- Article 6 of the Law of 19 December 2020
- Grand-Ducal Regulation of 14 November 2022 providing details on the Law of 19 December 2020
- Articles 33 (1), (2) & (3) and 39 (1) & (1a) of CSSF Regulation N° 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing

CSSF requested banks to have in place an adequate process that allows them to detect and report persons, groups and entities on targeted financial sanctions lists without delay after adoption or amendments of said lists by implementing processes ensuring:

- Handling of daily generated name screening/transaction screening alerts, at least by first level of control, without delay;
- The execution of the related restrictive measures, such as the freezing of related customer accounts also needs to be carried out without delay, even if the alerts need further investigations which take longer than 24 hours (which may take up to several days) to confirm the suspicion;
- Notification to the Ministry of Finance without delay, always with reference to a legal basis, and copy at the same time to the CSSF, even if the full investigation is not finalized.

Case study: Follow-up measures taken by the CSSF regarding the frequency of the name screening in order to detect persons, entities and groups subject to TFS and regarding the frequency of updates of these lists (i.e. UN, EU, national lists)

Following the review of data included in the 2021 Financial Crime Survey of the CSSF, it appeared that some information provided by a certain number of investment firms in relation to the frequency of name screening was not appropriate, including in matters of TFS lists.

In January 2023, the CSSF sent observation letters to the concerned investment firms requesting them to further explain the answers provided in the survey, to give details on their name screening process and to take all the necessary remedial actions in order to fully comply with the requirements in place:

[534] Natural persons, legal persons, BO.

- Law of 19 December 2020
- Articles 33 and 39 of CSSF Regulation N°12-02 of 14 December 2012 on the fight against money laundering and terrorist financing

Some of the answers, deemed unsatisfactory, led to the sending of injunction letters in order to emphasize the "without delay" requirement and enjoin the entities to take all the necessary remedial actions as well as to provide the CSSF with the deadline by which these remedial actions are to be taken.

Case study: Reprimands issued against two credit institutions following deficiencies identified in the TFS process

In 2024, the CSSF issued reprimands against two credit institutions following significant deficiencies in their respective TFS processes identified in 2022-2023:

- Late implementation of restrictive measures in financial matters towards two accounts held by one client impacted by Regulation (EU) No 269/2014, as amended, on which bank charges were automatically debited and interests credited monthly, but no funds were accessed by a person subject to restrictive measures in financial matters;
- Late information to the Ministry of Finance of the implementation of the relevant restrictive measures towards the accounts in question;
- Late implementation of restrictive measures in financial matters (such as the freezing of funds without delay) towards a person listed in Annex I of Regulation (EU) No 269/2014, as amended, and subsequently late reporting to the Ministry of Finance of the implementation of the relevant restrictive measures towards this person, which constitute a failure to comply with Articles 2 and 7 of the aforementioned (EU) Regulation, Article 6 (1) of the Law, Articles 1 and 2 of the Grand-Ducal Regulation of 14 November 2022, as well as Article 33 (2) of CSSF Regulation 12-02, which require that restrictive measures in financial matters be implemented without delay and also communicated without delay to the Ministry of Finance;
- Whilst initial screening was conducted, an absence of ongoing screening against the list of sanctioned persons in Appendix I of Regulation (EU) No 269/2014 as amended of several investors as well as of parties related to investors (including for example the beneficial owners or the representatives of a legal entity) in traditional and alternative funds for which the professional acts as transfer agent, and this during a number of months, which constitutes a breach of Article 3 of the Law, as well as of Article 33 (1) and (3) of CSSF Regulation 12-02 which foresee the obligation for the professionals subject to the Law to identify without delay the States, persons, entities or groups involved in a transaction or a business relationship subject to restrictive measures in financial matters;
- Serious deficiencies in the professional's organisation and internal control system leading to inadequate implementation of restrictive measures in financial matters and to failure to detect, upon regular controls, the above-mentioned breaches to the applicable legal and regulatory provisions, breaches that have continued for a number of months, which constitute a breach of Articles 38 (2) and 39 (1), (2), (6) and (7) of CSSF Regulation 12-02 which require the professional to put in place policies and procedures that cover all its obligations related to the fight against ML/TF, including those related to restrictive measures in financial matters, and to implement a complete and up-to-date customer database, while performing regular checks to ensure the proper functioning of this system.

6.4.1.5. Detection, reporting and outcomes

Professionals supervised by the CSSF must apply the required restrictive measures and inform the competent authorities without delay when states, persons, entities or groups are identified as involved in transaction or business relationship subject to prohibitions or restrictive measures in financial matters (article 33 of CSSF Regulation No 12-02).

Upon detecting true positive sanctions screening matches, supervised professionals are required to freeze associated funds without delay and report this to the MoF [535] (copying the CSSF). CSSF supervision of the effective implementation of financial restrictive measures may also include checks to assess whether reports submitted by supervised professionals are of the required quality, i.e. whether the report is relevant and contains full information.

The CSSF exchanges information with the MoF, and vice-versa, pursuant to the provisions of article 9 (2) of the Law of 19 December 2020.

In addition, true positive sanctions matches should also be reported to the CRF if there are specific suspicious elements relating to TF, ML or an associated predicate offence. It should be noted that failure to comply with restrictive measures as provided for by article 10 of the Law of 19 December 2020 is an associated predicate offence to ML. Generally speaking, CSSF-supervised professionals' understanding of this process has improved in recent years following exchanges between the professionals and the concerned authorities: in previous years, the CSSF's Banking Department had identified cases where the reports had been sent to the CRF instead of the MoF as a first instance. In these cases, the CSSF followed up with the professionals (e.g. via dedicated interviews with Chief Compliance Officers of the banks) to help improve understanding of their reporting obligations and ensure compliance with the requirements. Given its size, the financial sector under CSSF supervision presents the highest rates of true positive matches and reporting to the MoF (as well as implementing asset freezes).

CSSF-supervised professionals report regularly to the MoF funds and other assets frozen in compliance with several other TFS regimes (e.g. Libya, Syria, Tunisia, Yemen, Russia, etc.).

6.4.2. CAA

Stakeholder	Key responsibilities related to TFS for PF and TF
Other public authorities	
Commissariat aux Assurances (CAA)	• "Responsible for the supervision of natural and legal persons falling within its competence in the insurance sector for the purposes of the implementation of the Law of 19 December 2020 on the implementation of restrictive measures in financial matters. In accordance with the combined provisions of article 2, paragraph 2, and article 31 of the CAA Regulation 20/03 dated 30 July 2020 on the fight against money laundering and terrorism financing, these persons have to apply restrictive measures and inform without delay the competent authorities in financial sanctions matters. A copy of this reporting has to be addressed to the CAA."[536] • "Has the same powers as those conferred by Articles 8-2, 8-4, 8-5, 8-6, 8-7 and 8-9 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended"[537]

The CAA is responsible for the prudential and AML/CFT supervision of the insurance sector. It should be highlighted that even if not all entities under CAA supervision fall within the scope of 2004 AML/CFT Law[538],

[536] Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals*, 2021 (link)

[537] Article 6(5), Law of 19 December 2020 (link)

[538] See also the NRA for a detailed view of all CAA-supervised subsectors.

they all need to comply with international financial sanctions, including PF-TFS and TF-TFS, as all EU Regulations are directly applicable in Luxembourg. Pursuant to article 6(2) of the Law of 19 December 2020, the CAA is responsible for the supervision of the persons falling within its competence for the purposes of the implementation of said Law.

The CAA issued on 30 July 2020 the 2020 CAA AML/CFT Regulation which repeals the 2013 CAA AML/CFT Regulation. The main amendment relating to international financial sanctions (including PF-TFS) is that the regulation provides specific provisions which have to be applied by all natural and legal persons under the CAA supervision even if they do not fall within the scope of the 2004 AML/CFT Law.

The CAA monitors the effectiveness of processes and controls put in place by supervised entities to meet their obligations regarding both TF and PF-TFS. The CAA assesses the effectiveness of such measures across the supervisory lifecycle, including (1) at market entry, by conducting "fit and proper" assessments, (2) as part of ongoing supervisory activities (on-site and offsite), and (3) through efforts to promote understanding and risk awareness. The supervisory approach deployed by the CAA across its supervised entities is largely the same for any sanctions regime (no meaningful differentiation made across PF and TF TFS). In terms of supervisory approach, the CAA's AML/CFT department was as at December 2023 composed of 6 specialists providing support to the prudential departments on AML/CFT matters as needed.

The CAA is also a member of the Monitoring Committee for International Financial Sanctions.

It is important to note that requirements and supervision for insurance sector entities, as for the financial sector under CSSF supervision, relate to the implementation of TFS specifically. For TF more broadly, there are additional obligations and controls in place, included in the broader AML/CFT framework by the CAA and supervised professionals, which are described in the NRA. For PF, however, there are no specific requirements for risk-based monitoring of PF activity other than sanctions implementation, since PF is embedded in the Law of 19 December 2020. The obligations for PF and TF sanctions implementation that the CAA monitors are directly derived from the Law.

6.4.2.1. Market entry controls

The main market entry control for TFS relates to "fit and proper" procedures, which include communication obligations (such as on shareholder structures or entry into new markets) and sanctions screening checks.

The CAA put in place a "fit and proper" procedure which defines the checks carried out by the CAA with regard to the good repute and fitness of all natural or legal persons applying for a license or intending to perform a specific function under the supervision of the CAA (i.e. initial control). When the function is performed by a legal person, the CAA also checks the good repute of its representatives.

The CAA collects "fit and proper" files for the board members, the licensed manager, the branch managers (if any), the Solvency 2 key functions (actuary, risk manager, audit, compliance), the IDD key function (Insurance Distribution Directive) and the AML key functions. These files encompass detailed information regarding the background of the person (experience, studies…) to support its fitness as well as a criminal record, a copy of the ID and a sworn statement on the question whether the person has not previously been declared bankrupt. Cooperation with the national and international authorities is also part of the "fit and proper" procedure.

Sanctions screening performed by the CAA is done at market entry and includes shareholders, key function holders and BOs of the undertakings. A dedicated screening tool is used. No positive match has ever been found on a sanctioned person or entity. However, if a match is found, it must be reported to the AML/CFT department and the executive committee for further communication to the Ministry of Finance.

The CAA also applies market entry controls on entities licensed in Luxembourg establishing branches or providing services abroad. According to the law of 7 December 2015 on the insurance sector, as amended, the CAA can refuse the establishment of such branch or the provision of such services if the host state is subject to international sanctions or does not apply the international standards on combatting money laundering and terrorist financing. It is worth to note that any commencement of operations in a third country is subject to the CAA's prior authorization according to articles 133 and 139 of the law of 7 December 2015 on the insurance sector, as amended (conditions for establishment of a branch).

In addition, for reinsurers, the CAA has defined criteria that the ceding companies have to comply with, including that these ceding companies must be located in jurisdictions with a regulatory regime close to the EU standards. In any case, the provision of reinsurance services must not be prohibited by sanctions, embargoes or other similar measures at the request of the United Nations, the European Union or other international bodies that may pronounce themselves in favour of a partial or total embargo on the insurance and reinsurance sector. Moreover, the country where the cedant is domiciled must not be identified by the FATF as having deficiencies in the standards for the fight against money laundering and terrorist financing, in accordance with the Circular Letters published quarterly by the CAA. Typically, the kind of group that want to establish a captive in Luxembourg are well-established large companies (typically listed or regulated, primarily large companies in the EU), so the risk of reinsurance captives for shell or front companies is low. In 2021, the CAA did inform a company that wanted to apply for a license as a reinsurance captive that its application file was not in a condition to be submitted to the CAA board for an approval based on several reasons. Amongst them, there was the assessment that the ceding company was not considered to be subject to prudential rules deemed to be at least equivalent, as a whole, to the legislation applicable in the Member States of the European Union, as required by article 3 of CAA Regulation 15/03, and did not belong to a reputable international group.

Finally, the approval of a Luxembourg insurance and reinsurance undertaking is subject to the communication to the CAA of the identities of the shareholders or members, direct or indirect, whether natural or legal persons, who have qualifying holdings in that undertaking. At least once a year, the insurance and reinsurance undertakings inform the CAA of the names of the shareholders and members possessing qualifying holdings and the sizes of such holdings. Regarding the acquisition of shares, it is worth noting that any natural or legal person who has taken a decision either to acquire, directly or indirectly, a qualifying holding in a Luxembourg insurance or reinsurance undertaking or to further increase, directly or indirectly, such a qualifying holding in a Luxembourg insurance or reinsurance undertaking shall first notify its intention to the CAA. The CAA has therefore updated information regarding the shareholder structures of all the insurance and reinsurance undertakings under its supervision.

6.4.2.2. Understanding of TF/PF risks and related obligations

CAA-supervised entities have access to a **range of methods and sources** to ensure they understand their obligations relating to TF and PF TFS:

- **Circular Letters:** The CAA issued **Circular Letter 11/9 and Circular Letter 20/12** relating to international financial sanctions to remind supervised entities of their obligations and to recommend the subscription to the MoF's Newsletters. Moreover, following the Law of 19 December 2020 on the implementation of restrictive measures in financial matters, the CAA issued four informative notes related to this matter (i.e. 21/1, 21/5, 22/6 and 22/7). The CAA **publishes on a regular basis the latest FATF statements** concerning high-risk jurisdictions against which enhanced vigilance measures and, where appropriate, counter-measures are required and jurisdictions under increased monitoring of the FATF.
- The **2020 CAA AML/CFT Regulation** includes provisions to be followed by the supervised entities (please refer to articles 31 and 37). Supervised entities are required to implement such provisions in their internal policies. These provisions can be summarised as follows:
  - **Screening of the parties** involved in the relationship **against sanctions lists before** establishing a business relationship and **during** the relationship to ensure restrictive measures or prohibitions can

be applied without delay. It should be noted that the screening has also to be performed on the beneficial owners when the supervised entities fall within the scope of the 2004 AML/CFT Law. Nevertheless, supervised entities which do not fall within the scope of the 2004 AML/CFT Law have to take the appropriate measures if doubt exists on whether beneficial owners could be subject to restrictive measures in financial matters (please refer to the Comments of Articles (Article 2) related to the 2020 CAA AML/CFT Regulation).

  - **Screening of the transactions throughout the course of the business relationship**: screening has to be performed before any transactions on an insurance contract, regardless of the frequency determined by the professional based on its risk assessment.
  - The entities supervised by the CAA have to take the relevant measures **without delay** when they identify states, natural and legal persons, entities and groups subject to restrictive measures in financial matters. Furthermore, they have to inform the MoF. A copy of this communication has to be sent to the CAA at the same time.

- Together with the 2020 CAA AML/CFT Regulation, the CAA issued **Comments of Articles** which **clearly refer to the guidelines** published by the MoF.
- **The CAA website includes a dedicated page[539] on international financial sanctions which includes FATF guidelines over PF and a link to the website of the MoF**.
- **The CAA exchanges with supervised entities** as well as with the **insurance professional associations** about international financial sanctions. Further to such meetings, the Association des Compagnies d'Assurances et de Réassurances du Grand-Duché de Luxembourg (ACA), which represents the Luxembourg insurance and reinsurance undertakings, issued guidelines[540] for its members and the Association Professionnelle des Courtiers en assurance au Luxembourg (APCAL), which represents the brokers/brokerage firms, **took the relevant measures** to find specific dedicated tools in order to help the supervised entities to comply with their obligations.
- The AML/CFT department is the point of contact for supervised entities in relation to certain PF/TF matters, although supervised entities are aware of their obligations to resolve questions related to the implementation of financial restrictive measures, such as regarding homonyms, with the MoF.
- The CAA participates in and organises conferences where the topic of international financial sanctions is discussed. For instance, a webinar organized on 24 September 2020 by the CAA (295 attendees) included a specific session dedicated to international financial sanctions. Moreover, on 20 April 2021 two agents of the CAA were speakers at an event organized by IFE (one of the presentations was about international financial sanctions). On 28 October 2021, the CAA organized a conference dealing as well with matters related to the implementation of restrictive measures and financial matters (304 attendees). Finally, at the 2023 annual conference organized by the CAA (held on 11 October 2023 with 217 attendees), there was a dedicated session about the evolving legal framework applicable to international financial sanctions.

The CAA has conducted dedicated surveys on cyber risks and maritime risks for insurance subsectors in relation to PF, TF or TFS. No major deficiencies have been found.

6.4.2.3. Prevention/private sector controls

Supervised entities in the insurance sector are required to put tangible measures in place to fulfill the obligations described above, primarily via sanctions screening procedures (upon start and during a business relationship). P&I clubs (which constitute approximately 2/3 of maritime business) have particularly tight controls.

---

[539] Website of the CAA, accessed July 2025 (link)

[540] Website of the ACA, accessed July 2025 (link)

Moreover, additional guidance is provided to supervised entities falling within the scope of the 2004 AML/CFT Law on particular internal controls in this regard, based on the 2020 CAA AML/CFT Regulation:

- Art. 37(5): "*The supervisory system shall enable the professional to take rapidly and, where applicable, automatically, measures in the event of the detection of a suspicious activity or operation. The Compliance Officer is solely competent to decide on the application and extent of these measures and their termination, where applicable, in consultation with the Responsible for Compliance or the management.*"
- Art 37(7): "*The supervisory system shall be subject to an initial validation by the Responsible for Compliance and to a regular control by the Compliance Officer in order to adapt it, where necessary, to the development of the activities, the customers and the AML/CFT standards and measures.*"
- Article 36(2): "*The professional's AML/CFT policies and procedures shall cover all its professional obligations and shall include, where applicable, among others: procedures relating to financial restrictive measures.*"

The review of the annual accounts of all insurance undertakings and reinsurance undertakings is performed by an approved statutory auditor who is required to complete a distinct report which has to be sent to the CAA.

Since 2018, such report includes a dedicated question to check whether insurance undertakings and reinsurance undertakings put in place adequate measures to implement United Nations Security Council Resolutions and acts adopted by the European Union containing prohibitions and restrictive measures in financial matters against certain persons, entities or groups in connection with the fight against terrorism. In 2021, this question was amended following the entry into force of the Law of 19 December 2020 concerning the implementation of restrictive measures in financial matters. It covers all restrictive measures in financial matters.

While all life insurance undertakings (except one[541]) put in place the required measures in that respect, the table below demonstrates the percentage of non-life and reinsurance undertakings which took the required measures, showing a positive trend.

Table 26: Percentage of non-life and reinsurance undertakings having taken TFS implementation measures, 2019-2023

	2019	2020	2021	2022	2023
Non-life insurance undertakings	86%	87%	92%	89%	95%
Reinsurance undertakings	85%	97%	99%	99%	99%

Unlike life insurance undertakings, there is no distinct report for brokers. Therefore, no external check is performed to confirm that they put in place the relevant action to implement international financial sanctions. However, according to the information provided in the annual reporting (self-declaration), all brokers and brokerage firms confirm that they take the relevant actions to implement international financial sanctions, including therefore PF and TF TFS. Indeed, based on the qualitative questionnaire sent in 2022, 89 % of the brokers have acquired a screening tool allowing them to comply with the financial sanctions. The outstanding 11% provided the CAA with explanations regarding the reasons for the non-acquisition of a

541 While the required measures were in place in the previous years, the approved statutory auditor detected deficiencies in the screening system for one life undertaking in run-off in 2023. It, however, pointed out that mitigation measures were ongoing.

dedicated tool (e.g. nature and size of the activities do not require such tool). To compensate, they carry out manual checks against sanctions lists, conduct internet searches or take into consideration the Newsletters issued by the MoF.

P&I clubs and traditional commercial insurers active in the maritime sector declared to perform controls at new client onboarding and also throughout the client relationship (i.e. the period of coverage and at the payment of the insurance benefits). In particular, said insurers communicated to the CAA that they:

i. Have implemented risk management policies and operational procedures which detail, inter alia, the due diligence to be conducted over clients with regards to TFS and the treatment of the alerts
ii. Have adopted the following mitigation measures:
    – Exclusion of maritime flag
    – Exclusions of transported goods
    – Namechecking via automatic screening tool mostly on a daily or weekly basis and at trigger events (i.e. claims payment)
    – Third party report (special investigation)
    – Tracking solution (Concirrus, Windward, Informa, Geocollect…): AIS capability to track the ships in various areas (drawing alerts if for example ships go off-track, lose signal, etc.)[542]
iii. Screen the persons listed herein below against the sanction lists issued by the UN and EU:
    – Clients (e.g. policyholders or P&I members)
    – Intermediaries
    – Recipients of the compensation

Regarding especially P&I clubs which hold the majority of maritime sector insurance business and are deemed higher risk for TFS risk purposes, additional controls are done. The clubs have very strict policies in terms of sanctions, which they consider as one of the highest compliance risk in the P&I and shipping industries. Specific procedures, tools and training have been implemented to mitigate this risk. Notably, there is a due diligence process before accepting a new member to the club: the members are the policyholders of the entity and each new member is checked against different criteria encompassing its exposure to sanctions.

The claims are either paid to the policyholder of the contract or to the claiming third party in case of a liability cover, but no other party will receive money. The payments are made to a bank account; no payment is made in cash. Sanction checks are done at the settlement by each paying insurer. Additional controls are made before a claim is paid, namely:

- Analysis by a claims manager – opening and checking that the claim is covered by the insurance contract, i.e. analysis of the facts surrounding the occurrence of the claims against the guarantee/exclusions of the policy
- Setting up an opening provision (i.e. an estimation of the ultimate amount the claim will cost)
- Analysis of additional documents justifying the reality of the claim and the associated cost (repairment bills, expert's report…) – often provided after the early notification described in the first bullet point

[542] To be noted that, according to the answers provided to the maritime questionnaire launched by the CAA, tracking solutions have been implemented by all three P&I clubs and as well by the traditional commercial insurer which in 2020 had underwritten premiums related to the maritime business for an amount equal to 130 million EUR (i.e. 62% of the premiums related to the maritime business collected by traditional commercial insurers in 2020).

- Sanctions screening of policyholder of the contract or to the claiming third party of a liability cover
- Payments disbursement

Non-life direct insurers are structured in a similar way: claims managers receive a certain authority that allows them to analyse and settle claims up to a certain amount. If this amount is exceeded, the file is escalated to an upper level and the settlement of important amounts goes through several checks (four-eyes, etc.) before the money is transferred. Except for the very few simple cases, the steps described above will take place over an extended time period. Liability cases are often subject to litigation. On top of the four-eyes principle as described above (1st line of defence), another common feature between the non-life insurers is that the claim management is internally peer-reviewed (i.e. claims managers will review the file of their colleagues, based on a random selection, as 2nd line of defence) and subject to internal audit (3rd line of defence). This system of 3 lines of defence is largely in place for both entities with cross-border transactions and local carriers.

For reinsurers, generally, reinsurance premiums are paid by the ceding company or the reinsurance broker on the bank account of the reinsurer and claims are also paid via a transaction between the bank of the reinsurance undertaking and the bank of the ceding company (or its broker). No cash settlement is conducted. Further, no transaction is conducted with the primary policyholder: all transactions occur between the reinsurance and its ceding company as counterparty. That said, reinsurers are required to perform CDD checks on their ceding companies, which include sanctions screening. There are no legal obligations for reinsurers to ensure that ceding companies perform adequate CDD on their primary policyholders.

Although not a primary focus for this study, there are also additional measures in the life insurance sector, where it should be noted that the country of origin of the funds is a risk that the supervised entities have to consider in their ML/TF risk assessments. A specific question has been included in the annual quantitative questionnaire to be completed by all life insurance undertakings allowing the CAA to identify the life insurance contracts for which the client or another party of the contract has been identified as being on a list of international sanctions. The analysis of recent quantitative questionnaires (for financial year 2023) showed that the number of contracts in the life insurance market for which the client or another party of the contract has been identified as being on a list of international sanctions is very limited. It appears that only three life insurance undertakings have one client being on a sanctions list (i.e. OFAC).

6.4.2.4. Supervision and enforcement

The CAA monitors the effectiveness of supervised entities’ processes and controls through both desk-based and on-site inspections to ensure that they meet their obligations.

Table 27: CAA monitoring by entity type

	Type	Life insurance	Non life Insurance	Reinsurance	Broker
Desk-based	Compte rendu annuel (annual report) *Prepared by supervised entities*	✓	✓	✓	✓
	Distinct report *Prepared by approved statutory auditors*	✓	✓	✓	N/A
	Rapport Spécial *Prepared by approved statutory auditors*	✓	N/A*	N/A*	N/A
	Specific enquiry (i.e. maritime questionnaire)	✓			
On site	On site inspections (planned)	✓	✓	✓	✓
	On site inspections (trigger event)	✓	✓	✓	✓

*Except for non-life or reinsurance undertakings authorized to non-life insurance classes 14 (credit) and 15 (suretyship) listed in Annex I to the law on the insurance sector.

The CAA analyses the outcome of the annual distinct report issued by the approved statutory auditor for each insurance and reinsurance undertaking, which contains a specific question dedicated to the international financial sanctions. In the same manner, the CAA also analyses the annual reporting filed by the brokers/brokerage firms. In 2023, the CAA conducted a total number of 388 desk-based reviews.

The CAA collects data regularly from the industry, both AML/CFT specific and prudential. For example, the CAA collects data regarding risk location, i.e. the premium and the claims paid per risk location[543].

With regard to on-site inspections, TFS are embedded in the topics to be covered, particularly for international players. The verification on TFS is done by the prudential department on the basis of a questionnaire developed by the AML team or directly by the AML team itself. During on-site inspections, the CAA analyses the procedure and the effectiveness of controls in place in relation to international financial sanctions. For example, on-site inspections typically examine policies and control systems for sanctions screening.

27 on-site inspections on (re-)insurance undertakings englobing TFS were carried out in the 2021-2023 period.

It should be noted that the CAA has the authority and powers to supervise the effective implementation of TFS. As such, the CAA can control entities (including issuing sanctions, as required) if there are deficiencies.

6.4.2.5. Detection, reporting and outcomes

Entities supervised by the CAA shall apply the required restrictive measures and inform the competent authorities without delay when persons, entities or groups are identified as involved in transaction or business relationship subject to prohibitions or restrictive measures in financial matters (articles 31 and 37 of the 2020 CAA Regulation).

[543] The location of a risk is defined according to Art. 43 paragraph 17 of the modified law of 7 December 2015 on the insurance sector.

Upon detecting any positive sanctions screening matches, CAA-supervised entities are required to freeze associated funds without delay and report this to the MoF [544] (sending a copy of this report to the CAA). There is the MoF set template for doing so, and CAA-supervised entities typically also report in individual formats attaching any relevant documents. CAA does not review these reports before being issued, but it does include checks in its supervision activity to assess whether reports are being made to the required quality. In the context of this reporting, there is on-going communication between the MoF and the CAA-supervised entities regarding, for example, the applicability of the asset freeze in a given case, the conditions for receiving an authorization to use frozen funds, as well as several requests for authorization. Regular meetings between the MoF and the CAA-supervised entities to discuss developments of the related files are also held, either at the initiative of the MoF or following a request from the operators involved. The CAA also attends the Monitoring Committee for International Financial Sanctions.

The common practice followed by marine insurers is to terminate the insurance cover when there is suspicion of breach of international financial sanctions.

In addition, positive sanctions matches must also be reported to the CRF if there are specific suspicious elements relating to TF, ML or an associated predicate offence, it being noted that failure to comply with restrictive measures as provided for by article 10 of the Law of 19 December 2020 is an associated predicate offence to ML.

Luxembourgish insurance sector entities report regularly to the MoF funds and other assets frozen in compliance with several other TFS regimes (e.g. Libya, Syria, Tunisia, Yemen, etc.).

In turn, the CAA itself also has reporting obligations if its screening processes (e.g. as part of “fit and proper” assessments) identifies a positive match. To date, there has been no identified positive match.

[544] As laid out in the Law of 19 December 2020, Article 6(1): “*Natural and legal persons who are required to implement the restrictive measures provided for in this law shall inform the Minister responsible for finance of the enforcement of each restrictive measure taken in respect of a State, natural or legal person, entity or group designated in accordance with this law and the implementing regulations, including attempted transactions”.*

6.4.3. AED

Stakeholder	Key responsibilities related to TFS for PF and TF
Other public authorities	
Administration de l'Enregistrement et des Domaines (AED)	• "Responsible for the supervision of specific categories of persons referred to in art. 1 of the Law of 10 August 2018"[545] • "Has the same powers as those conferred by Articles 8-2, 8-4, 8-5, 8-6, 8-7 and 8-9 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended"[546]

6.4.3.1. Market entry controls

The following table gives an overview of the competent licensing authority for AED-supervised professionals.

Table 28: Licensing authority for AED-supervised professionals

<table>
<tr><th colspan="2">Regulated/Supervised professionals</th><th>Licensing authorities</th></tr>
<tr><td colspan="2">Casino</td><td>Government Council upon MoF recommendation submitted to the State Council for an opinion</td></tr>
<tr><td colspan="2">Real estate agents</td><td>MoE</td></tr>
<tr><td colspan="2">Dealers in precious metals and stones</td><td>MoE</td></tr>
<tr><td colspan="2">Accounting professionals</td><td>MoE</td></tr>
<tr><td rowspan="2">Trust and Company Service Providers</td><td>Business/Office centres</td><td>MoE</td></tr>
<tr><td>Professional directors[547]</td><td>AED[548]</td></tr>
</table>

The General Directorate for Small and Medium-Sized Enterprises of the Ministry of the Economy (MoE) is in charge of the licensing process of several professionals that are supervised by the AED, including real estate agents, dealers in precious metals and stones, accounting professionals and business centres. Besides the police record from Luxembourg and the last countries of residence (if the person has resided outside of Luxembourg in a 10-year period prior the request of the business licence), checks are done against the targeted financial sanctions lists.

In addition to the controls carried out by the MoE during the process of issuing the business licence, the AED carries out additional controls when registering professionals for VAT purposes. The AED has put in place control measures to minimise the risk of VAT fraud. Furthermore, these controls also mitigate the risk of professionals entering the market with criminal intentions.

The AED itself is responsible for demanding the registration of professional directors who are falling under the definition of a TCSP based on the Guidelines of the National Prevention Committee[549] and where they

---

[545] Ministry of Finance, *Guidelines relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals*, 2021 (link)
[546] Article 6(5), Law of 19 December 2020 (link)
[547] When the service provided meets the definition of article 1 (8)(b) of the 2004 AML/CFT Law.
[548] The AED conducts registration activity only, and on demand for professional directors. It does not conduct licensing activity.
[549] Guidance published in October 2021 and available here (link).

are not already registered with another supervisory body[550]. To aid this registration on demand, the AED has supported the MoJ to publish guidance on who can register and how professional directors can register.

Since 2022, the AED conducts fit and proper checks on professional directors by checking their ID documentation, criminal records and professional fiscal behaviour and screening them against TFS and PEP lists.

The tool used for checks is World-Check and, in case of a positive hit on the checks carried out concerning the TF and PF sanction lists, the AED would contact the MoF.

6.4.3.2. Understanding of PF/TF risks

As an AML/CFT supervisory authority, the AED is keen not only to inform professionals of their AML/CFT obligations but also to draw their attention to the importance of consulting the lists of international financial sanctions when they have to identify their client and/or the beneficial owner in accordance with their due diligence obligation.

It is for this reason that the AED has implemented a section on its website[551] dedicated to international financial sanctions, giving professionals the necessary tools to understand the issues at stake.

The professional is informed about the different sanctions regimes that exist at international, EU and national levels. The information also covers the national authorities competent in the matter, the expectations of the professional who must comply with international financial sanctions by specifying the links giving access to the lists of existing international financial sanctions for the UNSC and the EU, allowing the professional to verify the identity of his client and/or the beneficial owner within these lists.

Plans are underway to include specific references to PF or TF in the AED's AML/CFT risk assessment questionnaire, with questions referencing the checks that professionals conduct on clients and BOs through research tools and international sanctions lists.

6.4.3.3. Prevention/private sector controls

Professionals falling under the scope of the AED are DNFBPs with very often one-shot business relationships, which require them to properly identify their client and/or the BO at first contact. To this end, the identifications and verifications are made at the beginning of the business relationship and result not only in an identification by identity card, but also in additional searches on computer search engines (Google) available to the general public, in order to confirm the PEP or non-PEP profile of the customer and/or of the BO.

6.4.3.4. Supervision and enforcement

Since 2014, the AED also conducts frequent inspections to assess whether supervised professionals comply with their AML/CFT obligations. During onsite inspections, the AED is responsible for verifying compliance with professional AML/CFT obligations. Although these are not explicitly focused on TFS, they do cover some items which are relevant for PF or TF TFS, including:

- Customer due diligence – regarding client identification, identification of the BO, origin of funds and retention of documents;

[550] In these cases, the professional directors must provide evidence of the supervisor/SRB that they are registered with.
[551] Available here (link).

- Adequate internal organisation – including internal procedures, appointment of an independent AML/CFT manager/compliance officer, staff training and existence of risk analyses;
- Cooperation with AML/CFT authorities – particularly the existence of STRs submissions via the goAML portal, abstention from transaction execution when relevant and cooperation with the AED.

However, based on the Law of 19 December 2020, the supervisory authorities have the same powers as those conferred on them by articles 8-2, 8-4, 8-5, 8-6, 8-7 and 8-9 of the 2004 AML/CFT Law, as amended. As such the AED has the same legal capacity to control and sanction, as conferred by the 2004 AML/CFT Law.

6.4.3.5. Managing the Beneficial Ownership register for legal arrangements

The AED is responsible for the management of the BO register for legal arrangements (*Registre des Fiducies et des Trusts* or Register of Fiducies and Trusts). The bill of law addressing the operation of register for legal arrangements was voted on 26 June 2020 and was published on 10 July 2020. As such, the AED is responsible for the reception of data into the register and provides general information to concerned people (trustees) regarding their obligation to enter data of their trust contracts in the register. Concerned individuals are expected to register and, if there is any change in the fiducie or trust, submit a report within one month.

Where a natural person who is a Luxembourgish national is registered in the Register of Fiducies and Trusts, they must provide their nationality which is cross-checked. Otherwise, those accessing the data are required to report discrepancies or errors.

6.4.3.6. Mitigating factors related to the Freeport

The Luxembourg Freeport is subject to a robust regulatory and supervisory framework. Operators fall within the scope of the AML/CFT and TFS obligations applicable to professionals dealing with high value goods, including customer due diligence, beneficial owner identification, enhanced scrutiny of high-risk clients and jurisdictions, transaction monitoring, sanctions screening, suspicious activity reporting and cooperation with competent national authorities. The Freeport also applies strict access controls, inventory traceability measures, and systematic documentation of the movement of goods, supported by onsite supervisory activities performed by the competent authorities. The enforcement of targeted financial sanctions (TFS) is supported by established internal screening systems and formal escalation procedures.

Considering the comprehensiveness and effective implementation of the mitigation measures in place – particularly the stringent access controls, regulatory oversight, systematic CDD processes, sanctions screening mechanisms and the demonstrated cooperation with competent authorities – the residual risk associated with PF/TF/TFS misuse of the Luxembourg Freeport is assessed as low. The measures significantly reduce both the likelihood and the potential impact of misuse, and available supervisory evidence indicates a high degree of compliance across the sector.

In October 2018, a European Parliamentary Research Service case study focused on the controls at Luxembourg's Freeport. Relevant details from this include:

a. **Market entry controls**

To become a licensed Freeport operator in Luxembourg, an applicant has to provide, inter alia[552]:

- A lease contract, specifying the exact premises covered by the lease
- The company's articles of association; an excerpt of the trade register
- The authorisation of establishment from the MoE

[552] European Parliamentary Research Service, *Money Laundering and tax evasion risks of Freeports* (page 28), 2018 (link)

– A recent excerpt of the criminal record of the applicant and of people empowered to represent the company
– Last three balance sheets; a completed authorization request form and a commitment to regularly update and present said form to customs

b. Collection of Beneficial Ownership data

– Since July 2015, licensed operators have to identify who the ultimate beneficial owners of the stored assets are and keep this information on record[553]

c. Controls on goods entering/exiting the Freeport

– Goods can only enter the Freeport if the operators have notified customs and they have been cleared. This requires a mandatory physical verification by a customs officer[554]
– At the moment of exit, customs need to know the value, the owner (not the BO) and the destination of the goods

6.4.4. SRBs

Stakeholder	Key responsibilities related to TFS for PF and TF
Other public authorities	
Self-Regulatory Bodies (SRBs): *OAL/OAD, CdN, OEC, IRE, CdH*	• Responsible for the supervision of professionals within their respective competencies • "[Have] the same powers as those attributed to them by Articles 8-2a, 8-10, 8-11, 8-12 and 8-13 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended"[555]

6.4.4.1. OEC

The Luxembourg Order of Chartered Professional Accountants (OEC) was established under the amended law of 10 June 1999 on the organization of the profession of CPAs (the "1999 CPAs Law")[556]. The OEC supervises all CPAs approved in Luxembourg, covering both sole practitioners and legal entities of all sizes. It holds ongoing responsibility for AML/CFT oversight, which includes effective implementation of TFS, including for PF and TF, across the profession.

Complying with TFS is an integral part of a CPA's broad AML/CFT obligations. This compliance involves a thorough understanding and application of the requirements set out in the Law of 19 December 2020. Key obligations include performing name screenings, evaluating country risks, verifying the sources of funds and wealth, implementing Know Your Transactions (KYT) procedures, promptly notifying the Ministry of Finance in cases of confirmed matches, and maintaining ongoing cooperation with the relevant authorities.

The OEC has set out a comprehensive Professional Standard that outlines the obligations CPAs must fulfil, incorporating the provisions of the Law of 19 December 2020.

[553] European Parliamentary Research Service, *Money Laundering and tax evasion risks of Freeports* (page 30), 2018 (link)
[554] European Parliamentary Research Service, *Money Laundering and tax evasion risks of Freeports* (page 29), 2018 (link)
[555] Article 6(5), Law of 19 December 2020 (link)
[556] Website of the OEC (link)

The latest version of this standard, endorsed by the OEC General Meeting in 2023, requires CPAs to adopt robust measures to ensure compliance with all applicable laws and regulations, and with the Standard itself. These obligations include, but are not limited to, the following:

- implementing international resolutions relating to financial sanctions;
- requiring operators to inform the MoF about any prohibition or measure taken with respect to a natural or legal person, entity or group appearing on one of the lists published by the MoF in the context of the implementation of the aforementioned laws and texts.

To comply, CPAs must implement procedures that include verifying the identities of clients, beneficial owners and client representatives. A key component of these procedures is name screening these individuals and entities against the published sanctions lists.

6.4.4.1.1. Market entry controls

The MoE serves as the licensing authority pursuant to article 10 of the 1999 CPAs Law and article 3 of the 2011 Business Licenses Law. In this capacity, the MoE is responsible for conducting “fit and proper” assessments and issuing business licences. After the MoE has issued a business licence, each prospective new CPA must then approach the OEC to apply for registration pursuant to article 21 of the 2011 Business Licenses Law, prior to commencing its activities.

On receiving a registration request, the OEC must register this new member but may refuse registration under article 4 of the 1999 CPAs Law. Grounds for refusal include situations where the managers and employees are also employed by a non-CPA legal entity or when the corporate purpose is incompatible with CPA business. If unresolved, the OEC issues a letter to the MoE explaining the case, and shortly after the business licence is removed by the MoE and the information transmitted to the OEC.

Nevertheless, the OEC is responsible for identifying and verifying the structure of ownership (in case of a legal entity) as well as determining the UBO whilst ensuring that the majority of voting rights are held by CPAs, based on the documentation provided. Following this, the new legal entity or independent professional must be validated by the OEC Commission “Exercise of the Profession” (established pursuant to Chapter XI of the Internal Regulations).

The Commission, among other duties, verifies that the majority of directors are CPAs (article 10 paragraph 4 A) of the 1999 CPAs Law) and that the majority of voting rights are held by CPAs (article 10 paragraph 4 B) of the 1999 CPAs Law).

Upon validation, the OEC screens the names of legal entities, communications contacts and CPAs using a Dow Jones tool, which makes it possible to perform daily name screenings and ongoing monitoring (including against TF and PF TFS lists). If a potential match is identified, a memorandum is established and forwarded to the President of the OEC Board. There are possible outcomes: identification as a Politically Exposed Person (PEP), match with a sanctions list, or other issues such as adverse media. Each outcome triggers specific actions, including filing a report to the CRF (in case of suspicions of ML, associated predicate offence or TF) or reporting to other relevant authorities.

Screening is carried out daily and, since January 2020, Know Your Counterparty (KYC) and Know Your Transaction (KYT) procedures have been implemented throughout the membership period. These procedures involve risk assessments, thorough identification and verification of members and continuous monitoring of transactions. The aim is to prevent criminals or their associates from holding significant interests or managerial roles within CPA legal entities.

6.4.4.1.2. Understanding of TF/PF risks

The OEC communicates CPAs' obligations regarding TFS, PF and TF through a variety of channels, including a dedicated section on its website[557] that offers extensive resources, such as relevant legislation, FATF guidelines, EU and UN sanctions lists, and an AML/CFT guide, all designed to help CPAs comply with regulatory requirements and strengthen their internal AML/CFT procedures. Regular updates and detailed explanations are provided to ensure members remain informed about evolving obligations. These subjects are also addressed during on-site controls, at Annual General Meetings and in the OEC's Annual Report, reinforcing ongoing education and compliance within the profession.

Trainings are regularly offered to the CPAs that address AML/CFT, including TFS, sanction lists and name screening, transactions monitoring checks (KYT), and clear guidance on handling sanction list matches. Since 2015, both AML/CFT in-person and e-learning trainings have been available, provided by the OEC (through "AML days") and external partners, often at preferential rates for members. In addition, major firms and audit entities routinely conduct in-house AML/CFT training to their staff.

Additionally, the OEC distributes biennial RBA questionnaires to collect information about how CPAs implement risk-based AML/CFT measures, including name screening, due diligence, and transaction monitoring. High response rates indicate an general awareness and understanding of risks and compliance obligations. These questionnaires are updated regularly to reflect new legislation and emerging risks, such as those specific to TFS, PF and TF, and responses are used to gauge sector compliance.

Lastly, each CPA must complete an annual independence declaration that reiterates their obligations to comply with AML/CFT laws and requirements, serving as both a reminder and a compliance checkpoint.

6.4.4.1.3. Prevention/private sector controls

Based on the results of the 2024 RBA questionnaire, which reflects data collected from 2023, 95% of respondents confirmed that they perform name screening against mandatory sanctions lists. Additionally, 60% of those surveyed were found to have an adequate frequency of sanctions screening—a figure that has shown steady improvement in recent years.

6.4.4.1.4. Supervision & enforcement

The Board and the President of the OEC ensure that members uphold their professional duties in relation to AML/CFT compliance. Oversight of AML/CFT controls has been delegated to the COMCO ("*Comité Consultatif relatif à la LCB/FT*") as well as to designated AML/CFT controllers. The COMCO, comprised solely of CPAs, is principally responsible for validating reports prepared by the controllers and for communicating the results directly to the audited CPAs.

The OEC integrates TFS, PF and TF into its wider AML/CFT supervision and enforcement, utilising both off-site (RBA questionnaires) and on-site evaluations to assess the robustness of procedures and overall compliance. When instances of non-compliance are detected, the OEC initiates follow-up actions, which may include the creation of detailed action plans, the introduction of additional control measures and, where necessary, the initiation of disciplinary proceedings. Issues or initial shortcomings that are satisfactorily resolved are deemed closed once minor deficiencies have been rectified. Conversely, if controls remain insufficient, the OEC subjects the firm to enhanced supervision ("*contrôles rapprochés*") and, should shortcomings persist, may escalate the matter to formal disciplinary action, including issuing a summons before the President.

[557] Website of the OEC (link and link)

6.4.4.1.5. Detection, reporting and outcomes

The 2024 RBA questionnaire, which reflects data collected from 2023, included a specific question related to the number of reports issued to the MoF, as well as whether firms have written and specific procedures for reporting to the MoF. Between 2019 and 2023 inclusive, the OEC recorded a total of 18 reports related to TFS being sent to the MoF.

6.4.4.2. OAL/OAD

Within their self-regulatory power, the Ordres des Avocats (OAs) have included the provisions of the Law of 27 October 2010 in the legal and regulatory framework applicable to OAs and lawyers, through the Luxembourg Bar's AML regulation of 12 September 2018. Paragraph 59 (third indent) of this AML regulation provides that the measures deriving from international financial sanctions should be covered by the internal AML policy and procedures adopted by law firms:

> *"The procedure for on-boarding and monitoring business relationships; this should allow it to detect in particular people at high risk (politically exposed persons, persons or entities concerned by prohibitions or restrictive measures in financial matters), funds from or to destination of persons targeted by prohibitions or restrictive measures, or of countries which do not apply - or insufficiently apply - AML/CTF measures under the FATF declarations, as well as complex or unusual transactions."*

OAs plan to review their AML/CFT professional standard to further develop the professional obligations of law firms in relation with international financial sanctions. It is intended that new OAs professional standard – be it included in the AML regulation or subject to a specific regulation – will be more detailed and include additional provisions about this specific topic.

6.4.4.2.1. Market entry controls

In terms of market entry controls, OAL/OAD are responsible for licensing and registering members. For every supervised lawyer, sanctions screening (as well as other screening more specific to AML topics) is conducted on market entry or re-entry and reviewed annually, in January of each year. To date, there have been no instances of lawyers being subject to TFS for TF or PF. It is also mandatory that a recent criminal record from Luxembourg and/or the country of provenance is provided to the Luxembourg Bar by all candidates before being accepted. It is also mandatory that any lawyer who has already been registered with another bar provides official documents signed by the Bar of origin stating that she/he has no disciplinary record.

All lawyers are also controlled within the limits imposed by EU directive 98/5/CE of 16 February 1998:

- A lawyer is prohibited from practising any incompatible activities in regard to his/her profession such as among others the management of commercial companies, thus limiting the risks such activities would present[558];
- It is mandatory that trainee lawyers will be supervised for at least 2 years (minimum training period) by an experienced lawyer at least fully qualified for a minimum of 5 years as an "*avocat liste 1, avocat à la Cour*". Trainee lawyers are not allowed to establish themselves at another address than their supervisor during their training;
- Employers are allowed to ask their future employee to provide them with a recent copy of his or her criminal record;
- The Bâtonnier (president of the Bar) has to be informed of any court case directed against a lawyer. This includes all matters even of a private nature, not only civil and criminal cases. Criminal cases are also

[558] Article 1, Law of 10 August 1991 related to the profession of lawyer.

notified to the Bar through the services of the criminal courts or the services of the Attorney General or the Public Prosecutor. Any criminal case directed against a lawyer leads to the automatic opening of a disciplinary case;

- The Bâtonnier is also automatically informed of any search (warrant) at the office of a lawyer directed against the lawyer him or herself, respectively his or her client. The Bâtonnier is also informed of any hearing of a lawyer by the police or investigating judge. If the hearing is in regard to a criminal case or if a warrant is directed against the lawyer, a disciplinary procedure is automatically opened;
- The Bâtonnier is also informed of the seizure of any professional and private property of a lawyer if he or she fails to pay his or her debts. Disciplinary action is also regularly taken on those grounds;
- If a lawyer fails to pay his or her annual membership to the Bar or fails to prove the existence of a sufficient infrastructure, a simplified procedure will result in the swift removal of the lawyer from the Bar. The Bâtonnier can also request through the Attorney General the assistance of the police in investigating certain disciplinary matters.

Alongside the limits referenced above, there are several steps in the market entry and ongoing monitoring process for OAL/OAD members:

1. Every lawyer registered at the Luxembourg Bar is checked for good reputation at the time of his/her first registration at the Bar and at a subsequent re-registration (if any);
2. Pursuant to article 34 of the law of 10 August 1991 on the profession of lawyers, as amended (the "LPA"), lawyers may exercise their profession together either in the form of unincorporated partnerships or in the form of a company incorporated under Luxembourg or foreign law;
3. In each case, all partners or holders of shares or interests must be lawyers registered at the Luxembourg Bar or at another EU bar. The Conseil de l'Ordre (council of the Luxembourg Bar) may recognise non-EU bars as equivalent (for the purpose of admitting foreign registered lawyers as partners) under the condition that lawyers at such non-EU bars have conditions for registration, exercise of their profession and of partnership equivalent to those applicable in Luxembourg. To date, only solicitors registered at the Law Society of England and Wales and subject to the Solicitors Regulation Authority have been recognised as equivalent and then only as members of a recognised body (as opposed to licensed bodies).

Article 34 of the LPA thus establishes a strict prohibition in Luxembourg of non-lawyer ownership:

1. In January each year, law firms, whether organised as partnerships or companies, must send to the Bar a confirmation of independence where among others compliance with the principle of non-lawyer ownership and compliance with the requirements for independence as set out in the circulars no 3 (2018/2019) and no 1 (2021/2022) are checked. At that time, another compliance check (including against UN and EU sanctions lists) is made (i) on all partners or holders of interest of every law firm and (ii) on all single practitioners registered with the Luxembourg Bar.
2. The annual check guarantees a full good reputation control of all individual registered lawyers including holders of interest in law firms who are registered with the Luxembourg Bar. A law firm registered on list V of the Bar must have at least one holder of interest registered on list I of the Bar and exercising a significant influence on the affairs of the Luxembourg law firm. A law firm registered on list VI must have at least one holder of interest registered on list I or list IV of the Bar and exercising permanently in Luxembourg. In addition, for every law firm registered as a company on either list V or list VI of the Bar, it is a legal requirement that the members of the managing bodies are also holders of interests in the law firm concerned.

These rules ensure that law firms organised as companies are managed by Luxembourg registered lawyers, who control the affairs of the law firm and are screened for good reputation. Since 2022, the annual control described above requires that members of the management bodies of law firms provide a confirmation from their law firm that these members are of good professional reputation and have not been subject to any adverse proceedings.

6.4.4.2.2. Understanding of TF/PF risks

Several mechanisms are used to inform entities of their obligations regarding TFS for TF/PF:

- Firstly, publications on the OAs' intranet (and the OAL's public website[559]) include the applicable laws and regulations, the obligation to inform the MoF about prohibitions or restrictive measures taken against the persons, entities and groups included in the published lists. It also includes a link to the websites of the MoF and the CSSF. Links are also provided to the EU and UN sanctions lists themselves and updated, as required;
- In November 2021, the annual AML/CFT questionnaire covered 10 questions related to PF or TF risk factors. Based on this, a further offsite survey was conducted to understand – where there could be higher risk of TF or PF – individual firms' exposure to PF and TF;
- OAs training programs conducted by the OAL include this specific topic.

6.4.4.2.3. Prevention/private sector controls

The OAL has recommended the use of "Smart-Oversight", a KYC and AML streamlining process. This tool was adapted and a partnership was offered to the members of the Bar in November 2019. The tool allows browsing through the official list of sanctions, negative media and offers a machine learning algorithm reducing false positive results. Since then, the OAL has acquired the Dow Jones Factiva tool and has set up a partnership for the members of the Bar. Based on the November 2021 OAL off-site questionnaire, 100% of firms conduct sanctions screening, including 30% who use an automated screening tool. Moreover, 100% report having higher-risk policies in their internal AML/CFT manual (to the extent they accept to conduct higher risk activities).

6.4.4.2.4. Supervision & enforcement

The annual AML/CFT questionnaire is used to support the OAL's risk-based supervisory approach. As of November 2021, several questions in a dedicated section relate to TF/PF risk. In addition, since 2021, where the AML/CFT questionnaire flags that lawyers engage in TCSP activities, additional questionnaires are used to obtain further information on this topic, with questions focused on the type of TCSP activities provided, their internationality (to ascertain geographical risk) and the turnover associated with them. The purpose of this is also to support the OAL's controls and risk-based supervision.

For several years, the Conseil de l'Ordre of the OAL has performed on-site inspections to ensure that law firms respect their AML/CFT obligations and have implemented appropriate procedures and measures. Law firms, which are selected on a risk-based approach (including, for instance, whether the firm services TCSPs or have PEPs as clients or BOs), are to be also monitored for the specific topic pertaining to international financial sanctions, even if their activities fall outside the scope of the 2004 AML/CFT Law. At least one general off-site inspection is conducted per year as well as several sub-sectoral off-site inspections. In addition, on-site inspections are also carried out twice a week by the Commission de contrôle du Barreau de Luxembourg of the OAL. The objective of an on-site inspection is to control, on the basis of a control questionnaire, the law firm's compliance with its professional obligations arising from the AML/CFT legislation and professional standards. These controls necessarily include a review of the AML/CFT policies and procedures, including global risk analysis, as well as the control of their proper application on the basis of a sample of client files. For example, a review is conducted of firms' internal definitions of risk. Inspections

[559] Public website of the OAL (link)

include specific tests to ensure that law firms comply with the provisions of laws and regulations on international financial sanctions, as for example:

- The proper application of enhanced due-diligence measures in case of “*countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations*”;
- The implementation of “name filtering” on clients/representatives/respective beneficial owners and the tools or means put in place by law firms.

6.4.4.2.5. Detection, reporting and outcomes

As per the Law of 19 December 2020, natural and legal persons who are required to implement the restrictive measures in Luxembourg (including professionals supervised by the OAL and OAD) must inform the Ministry of Finance without delay of the enforcement of such restrictive measures. During the 2021-2022 judiciary year, there were 3 notifications to the OAL (respectively to the Ministry of Finance) of OAL members having implemented restrictive measures including freezing assets.

6.4.4.3. IRE

As indicated in the NRA, responsibility for licensing and registration for the audit profession is within the competence of the CSSF, whilst the IRE is responsible for ongoing AML/CFT supervision including restrictive measures in financial matters.

The IRE’s Professional Standards state that “*audit firms must be able to demonstrate, even if AML/CFT simplified due diligence measures are applied, that reasonable measures have been put in place to ensure compliance with the laws and other texts applicable to them and which are aimed at implementing international resolutions on financial sanctions”.*

“These reasonable measures include at least:

a. *The implementation of written internal procedures, proportionate to the nature, specificities and size of the audit firm, which include at least:*

- *The appointment of a person responsible for legal and regulatory monitoring and for following up on published lists of financial sanctions;*
- *The practical procedure to be followed in the event of an obligation to inform, without delay and without prior notification, the minister of finance of the implementation of prohibitions or restrictive measures taken against a state, a person (natural or legal), an entity or a group designated by the laws, regulations and other texts relating to the implementation of restrictive measures in financial matters and other financial sanctions, including attempted transactions;*
- *Checking the customer base and screening names against published lists of financial restrictive measures and other financial sanctions (hereinafter "sanctions lists"), as soon as they are published. These checks should cover at least the names of clients, beneficial owners and any person purporting to act for or on behalf of the client. In certain higher-risk situations, checks on the names of other parties involved in the transaction may be considered;*
- *The documentation of the verifications carried out;*
- *Where appropriate, arrangements for reporting to the firm's management information and results of verifications that may lead to the prohibition of the provision of certain services and to informing the ministry of finance;*
- *Training and other measures taken by statutory auditors and audit firms to ensure that their employees, including members of the management bodies and effective management, are aware of the provisions adopted in respect of restrictive financial measures and other financial sanctions;*

– *The application, where appropriate, of these specific procedures to the foreign branches of the audit firm.*

b. *Consulting the list of countries subject to financial restrictive measures and verifying the client, beneficial owners, persons purporting to act on behalf of or for the client and other parties involved in the transaction, from a database of persons, entities or groups included in published sanctions lists (name screening). The statutory auditor ensures that the lists he or she uses are up to date.*

c. *Informing the ministry of finance of the statutory auditor's execution of each restrictive measure taken in respect of a state, natural or legal person, entity or designated group, including attempted transactions".*

The IRE supports statutory auditors' understanding and implementing of these obligations and conducts posterior controls to ensure adequate procedures for screening clients on a regular basis are in place. There are several channels used to inform statutory auditors of these obligations regarding PF and TF TFS. Firstly, there is a dedicated IRE webpage[560] which describes the applicable laws and regulations on international financial sanctions, including the obligation to inform the Ministry of Finance about prohibitions or restrictive measures taken against the persons, entities and groups included in the published lists, etc. It also includes a link to the websites of the MoF and the CSSF. The IRE also publishes "Frequently Asked Questions" available on the IRE's website[561]. The purpose of FAQ is to provide additional information on practical aspects encountered by audit firms in the implementation of the legislation and the professional standards regarding AML/CFT and international financial sanctions. Lastly, the topic on TFS obligations is included in the IRE's training programmes. Training obligations are regulated by CSSF Regulation 16-10, including an expectation that all professionals conduct 8 hours of AML/CFT-related training every 3 years, including sanctions-related training. The first sanctions-specific training module has been held on 2 December 2021[562]. The IRE's yearly training programme[563] also includes a module called "Fight against money laundering and terrorist financing" which provides a detailed overview of the legislation in place in Luxembourg including restrictive measures in financial matters.

The risk linked to ***"countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations"*** (including TF and PF) has been specifically considered in the IRE's RBA analysis when defining the term "risky country". The 2019/2020, 2020/2021, 2021/2022 and 2022/2023 IRE annual reports**[564]** presented to the IRE General Assembly in June 2020, respectively in June 2021, June 2022 and June 2023 describe more broadly the key ML/TF risks identified for the audit profession.[565]

This risk-based analysis was performed by using information provided by audit firms in a specific questionnaire ("RBA questionnaire"). As an example, the RBA questionnaire provides some statistics on

[560] Section on International financial sanctions of the website of the IRE, accessed July 2025 (link)

[561] IRE, *FAQs*, accessed September 2024 (link)

[562] The learning Outcomes are: (1) Understand the complexities and innovation of techniques employed by criminals and rogue Government agents regarding the offences of money laundering, trade-based money laundering and proliferation finance, and why they pose such a serious problem, (2) recognize common red flags to detect trade-based money laundering and proliferation and (3) review trade-based laundering cases, identify risks & vulnerabilities, look at methodologies, tactics, and red flags, as well as proliferation and sanctions case studies.

[563] The 2022 training program included modules such as "Fight against money laundering and terrorist financing", "International financial sanctions - Overview of the legislation", "AML/CFT International standards – What you need to know", "Spotlight on corruption, insider threat – Are You Aware, Are You Prepared ?", "Compliance challenges in AML/CFT – Regulation is opportunity", "Emerging Threats – Cryptocurrencies, mobile money, securities & data challenges", "Fight against corruption" and "Sanctions and proliferation finance - Practical issues". The 2023 training program included modules such as "Fight against money laundering and terrorist financing", "Fight against corruption", "Cryptocurrency and criminality", "Fraud and Cyber fraud", "International financial sanctions"…

[564] IRE, *Rapports d'activité*, accessed July 2025 (link)

[565] Including TFS. This started with the 2019/2020 IRE activity report (pages 3, 19, 21 and 25) (link). It has been strengthened with the 2020/2021 activity report. The IRE has implemented new specific controls on that matter.

country of location of clients and their beneficial owners, the location of services provided, but also on the implementation of "name screening" by audit firms.

As of April 2024, all the audit firms declared that they use a "screening tool" to verify the names of clients, their representatives, beneficial owners, etc. involved in the business relationship, against sanction lists.

The "Frequently asked questions"[566] document on the IRE's website includes a section dedicated to TFS and the minimum controls and internal procedures expected of professionals:

- The implementation of specific written internal procedures regarding TFS;
- The designation of a person, within the audit firm, responsible for legal and regulatory monitoring and follow-up of the lists published ("TFS lists");
- The verification of the statutory auditor's "client base" in relation to the TFS lists (verification of clients and representatives, beneficial owners) ("name screening");
- The reporting of information (results of verifications, etc.) to the audit firm's management or to the compliance officer;
- The implementation of procedures to be followed in the event of an information to the MoF on the implementation of prohibitions or restrictive measures taken against a state, a natural or legal person, entity or group designated in accordance with the law, regulations or other texts relating to the implementation of restrictive measures on TFS, etc.;
- The subscription to the Newsletters of the MoF and of the CSSF to ensure the receipt of the information, etc;
- The training and other measures taken by audit firms to ensure that their employees are aware of the provisions of laws and regulations in relation to TFS.

The RBA questionnaires provide statistics which are used to monitor the effectiveness of statutory auditors' processes and controls to ensure that they meet their obligations in relation to TFS. As well as this, for several years, IRE has performed on-site controls to ensure that audit firms respect their AML/CFT obligations and have implemented appropriate procedures and measures. As of 31 December 2023, audit firms were selected based on a risk-based approach and were at least subject to a "full"[567] onsite control every six years. Control programmes include specific tests to ensure that audit firms comply with the provisions of laws and regulations on international financial sanctions and were updated to align with the minimum controls expected of professionals with regards to TFS. Checks include:

- The proper application of enhanced due-diligence measures in case of countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations
- The implementation of "name screening" on clients, their representatives and "beneficial owners"

Since the implementation of the Law of 19 December 2020, the IRE has not identified any sanctions infractions as part of its controls and onsite programme. However, there have been some preventative measures and follow-up controls requested.

[566] FAQ 2021-15, *Questions/réponses relatives à la législation et aux normes professionnelles en matière de lutte contre le blanchiment et contre le financement du terrorisme et à la mise en œuvre de mesures restrictives en matière financière*, abrogated and replaced by the FAQ 2023-0,1 *Questions/réponses relatives à la législation et aux normes professionnelles en matière de lutte contre le blanchiment et contre le financement du terrorisme et à la mise en œuvre de mesures restrictives en matière financière*.

[567] The objective of "Full scope" controls is to control, based on a control questionnaire, the audit firm's compliance with its professional obligations arising from the AML/CFT legislation and professional standards. These controls necessarily include a review of the AML/CFT policies and procedures, as well as the control of their proper application based on a sample of client files.

6.4.4.4. CdN

Notaries are subject to strict market entry controls, with only 36 notaries in office at any one time. They are appointed on the basis of seniority by the Grand Duke, and are characterised by their impartiality, independence and high levels of professional qualifications[568]. “Fit and proper” checks have been conducted on all new notarial candidates since 2020, which has involved all new notarial candidates being reviewed with respect to Police records, as well as subject to a sanctions screen (using Thomson Reuters). Any positive matches would result in the application being rejected. In addition, it needs to be stressed that notaries are appointed following the opinion of the CdN and of the General State Prosecutor[569]. In 2023, the Law of 7 August 1976 on notaries was amended and completed by a detailed description of the General State Prosecutor’s tasks[570]. Potential criminal backgrounds of candidate notaries are checked by the General State Prosecutor who conducts a check on the basis of the candidate's criminal record. Since 2020, the CdN carries out name check controls both on acting notaries as well as on candidate notaries applying for a vacant notarial post. This includes screenings against several sanction lists, which take in particular into account United Nations Security Council resolution designations and EU sanctions lists.

Notaries are informed on the topic of TFS via CdN Circulars and via the CdN’s website, which every notary in Luxembourg is invited to consult regularly. As part of its communication efforts, the CdN has also recommended to the Luxembourg notaries to verify the information available on the website of the Ministry of Finance and to subscribe to the newsletter of this Ministry. Furthermore, the CdN provides TFS as well as general AML/CFT awareness raising within the framework of continuous training sessions. The CdN organised one training session in 2021 and three sessions in 2022. Within the framework of these training sessions, participants received also updates on TFS issues.

Every notarial office has access to the Thomson Reuters/Refinitiv (TRR) database where sanction lists are stored and updated on an ongoing basis. Acquired in 2019, the TRR tool replaced another AML/CFT tool that the Luxembourg notaries had been using for numerous years under the same conditions. Having analysed various AML/CFT tool providers throughout 2018/2019, the CdN decided to replace the existing tool by the TRR tool. It is financed by the CdN on a multi-annual agreement.

For notaries, a simple check of their customer tool as part of their AML processes within the TRR platform allows every notarial office to screen respective customers against sanction lists. The CdN’s annual AML/CFT questionnaire, to which every notary has to respond, also highlights that the TRR tool covers the entire Luxembourg notariat.

The verification of the systematic use of the tool by the notarial offices forms part of the on- and off-site AML/CFT inspections of the notarial offices carried out by the CdN.

As of November 2022, sanctionable shortcomings had not been detected by the CdN. In case of such shortcomings, the CdN would apply the Law of 19 December 2020, as laid out in its article 6(5)[571].

---

568 CdN website (link) and Luxembourg, *National Risk Assessment*, 2020.

569 Article 16(1) of the Law of 9 December 1976 on notaries (as amended in 2023*)*.

570 Article 16 of the Law of 7 August 2023.

571 Article 6(5) of the Law of 19 December 2020: “*The competent bodies within the self-regulatory bodies have the same powers as those attributed to them by articles 8-2a, 8-10, 8-11, 8-12 and 8-13 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended*”.

6.5. Other authorities/administrators

6.5.1. OCEIT

Stakeholder	Key responsibilities related to TFS for PF and TF
Other authorities/administrators	
OCEIT	• "Competent authority for issuing authorizations for transactions such as the export, transfer, transit, technical assistance, brokering, and import of listed defense-related items, dual-use items and torture-related items; also grants derogatory authorizations for items of a strictly civilian nature within the framework of economic restrictive measures; the Political Affairs Directorate further has co-decision power concerning export autorisation for dual-use items and defense-related items"[572] • Has no specific competencies related to TFS for PF and TF.

OCEIT has competence for the granting of export licenses related to several types of items that may be subject to restrictions. These can be categorised into defence-related products, torture goods, dual-use items and civilian goods[573].

Licenses (and so applications) can be either individual or global in scope and, for dual-use items, EU general authorisations are also in place. Global licenses are usable for multiple transactions, on the basis that the company has adequate processes in place (an Internal Compliance Programme) in line with EU recommendations to conduct controls on export activity. Between 2018 and 2020, 33 global licenses were awarded for third countries, all for dual-use goods, at a total value of €47.6 million. OCEIT consults European legislation to check if there are specific items under authorisation for export/import prohibition related to economic sanctions.

Irrespective of whether an operator holds a global or individual license, companies are also expected to conduct "risk assessments" over the final destination person/entity themselves. If an operator has concerns about an export, they should not proceed further with their transaction and address those concerns with OCEIT. OCEIT can support them for further risk assessment which they automatically do for any new end-user that is also unknown to OCEIT.

When applying for a license, operators are expected to send all complete files as requested by the regulation for export activity, to be analysed by OCEIT. Application forms in the dossier are standardised. Applying companies write details of transactions and justify why they want to proceed with the transaction. A series of supporting documents for exports (detailed explanatory letter of the operation, end-user certificate; invoice/pro forma invoice, in some cases a sales agreement, and a recent extract from RCS) are mandatory to be submitted alongside the application form.

Export officers then analyse each application. Sanctions screening is also carried out by the company requesting the license. The application will be processed within 60 working days from the day the file is complete. The individual authorisation is valid for 1 year, the global authorisation is valid for 3 years[574]**.**

For all items (except for civil goods) or for all countries, including those in the scope of this report, OCEIT requires signature on licenses granted from two directorates of the MoFA.

[572] Provided by OCEIT.
[573] Definitions available on the Luxembourg government website (link).
[574] Further information available here.

The table below shows the licenses granted for all third countries between 2018 and 2020, as well as their value.

Table 29: Number of export licenses granted for all third countries, 2018-2020

		Dual use items	Military items
2018	Number of licenses	106	7
	Value	€3,701,000	€85,266
2019	Number of licenses	160	16
	Value	€773,000	€3,556,535
2020	Number of licenses	94	11
	Value	€6,186,000	€9,701,836

The interministerial export control working group which inter alia considers if adaptations are needed on legislation and discusses potential cases (especially in high-risk countries) meets quarterly on average. The group consists of members from the Ministry of State, the MoFA, the Customs Administration, the MoJ, the MoE and the MoF.

6.5.2. ADA

Stakeholder	Key responsibilities related to TFS for PF and TF
Other authorities/administrators	
Administration des douanes et accises (ADA)	• "Competent authority for the control of the physical transport of cash entering or leaving the Grand Duchy of Luxembourg as well as for the control of cash entering or leaving the Union"[575] • Competent authority for the levy of customs and excise duties • Competent authority regarding the control of any goods entering/exiting the Freeport, levying duties on these goods if applicable[576] and granting the authorisation for economic operators to establish their business within the Freeport[577]

The Administration des Douanes et Accises (ADA) is one of the three tax authorities under the MoF in Luxembourg. Aside its competency relating to safety and security, the ADA is in charge of levying customs and excise duties. The ADA does not hold competence for the implementation of TFS but does have an indirect contribution to sanctions implementation, given its competency relating to exports and imports of goods from and to Luxembourg.

For the movement of goods where customs control may apply[578], customs controls are based on a risk analysis according to the provisions of the Union customs code[579] and the Customs Risk Management Framework laying down common risk criteria and standards[580]. In case of a hit, the ADA reviews the documentation relating to the goods ahead of the export/import. The control of the goods can either be

[575] Law of 16 July 2021 (link)
[576] Article 243 and onwards, Union Customs Code (link)
[577] As of December 2023, there were 5 authorised freeport operators.
[578] Union goods are in free circulation within the EU.
[579] Articles 46 and 50, Union Customs Code
[580] Commission implementing decision (C(2018)3293 final) is not available to the public and is only made available for customs risk management experts in the Member States.

purely document-based, or document-based and physical. The physical control can only take place once the goods are presented to the ADA.

Regarding specifically dual-use goods, the same procedure described above applies to export and transit of such goods[581]. Additionally, in the same context, ADA carries out monthly post release checks on export declarations from sensitive operators based on lists received via the interministerial working group regarding the controls on export.

An internal database of the ADA, TARLUX, links goods based on their commodity code to the relevant sanctions regulations and other regulations that set conditions/restrictions on goods for both import and export.

In the example of DPRK and diamonds (excerpt below), for instance, TARLUX indicates that the goods are under general export prohibitions related to DPRK.

TARLUX[582] allows not just the ADA but also customs representatives[583] and other interested parties to verify the conditions and measures related to the import or export of specific goods with specific destinations, e.g. requiring an export license or for which a general prohibition applies (such as for the example of diamonds for DPRK), or to verify fiscal or commercial measures, among others.

Moreover, the ADA is one of the designated members of the interministerial export control working group, where designated authorities exchange about particular traffic relating to export and operators which may have given rise for attention.

Figure 7: Excerpt of TARLUX database for diamonds[584]

Origin	Start date	Measure type	Footnotes	Geographical area	Excluded countries	Duty expression	Conditions	Additional code	Regulation	Quota order no.
	28/06/2018	Export prohibition (278)	TM528	North Korea (Democratic People's Republic of Korea) (KP)					R1509/17	
	01/01/2007	Restriction on export (476)	CD354	All third countries (1008)			View conditions		R2368/02	
	28/06/2018	Export control on luxury goods (718)	CD223 TM684	North Korea (Democratic People's Republic of Korea) (KP)			View conditions		R2062/17	
	01/01/2008	Supplementary unit (109)		ERGA OMNES (1011)		Carats (one metric carat = 2 x 10^{-4}kg) (CTM)			R2658/87	

The ADA also plays a role in controlling the movements of goods in and out of the Freeport. To do so, a national database dedicated to supervised goods entering and leaving the free zone has been developed by ADA and is mandatory for all operators authorized to use the Freeport. Customs officers review goods entering and exiting the Freeport, as well as instances where property is transferred within the Freeport.

Lastly, the ADA also has the authority to retain undeclared or undisclosed cash equal to or above €10,000 at the border for a maximum of 30 days, which can be extended to a maximum of 90 days if deemed necessary and proportional according to EU Regulation 2018/1672[585] and the law of 16 July 2021 on cash control.

581 Article 1, Regulation (EU) 2021/821 (link)

582 Section "Services en ligne - Douanes – Luxembourg" of the public.lu website (link).

583 A customs representative is an economic operator offering customs formalities services to clients.

584 Specifically: diamonds, whether or not worked, but not mounted or set; nonindustrial, unworked or simply sawn, cleaved or bruted (CN code 7102 31 00).

585 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 (link)

6.5.3. LBR

Stakeholder	Key responsibilities related to TFS for PF and TF
Other authorities/administrators	
Luxembourg Business Registers (LBR)	• Mission to "manage and to develop the different registers it may be entrusted with by law, under the authority of the Minister of Justice"[586], including: - RCS (since 23 January 2003) - RESA (since 1 June 2016) - RBE (since 13 January 2019)

The primary mechanism used to manage the risk associated with legal persons in a centralised manner are the RCS and RBE as official registers maintained by LBR. The RCS requires all entities listed in the 2002 RCS Law to register their activity, annual accounts and natural and legal persons as shareholders and managers (*mandataires*), upon set-up and on an ongoing basis (including for any updates of initially submitted data). The RBE requires legal persons listed in the Law of 13 January 2019 instituting a register of beneficial owners to register their beneficial owners (as well as any updates to information on those beneficial owners). More details on the registers can be found on LBR's website, in the 2020 and 2025 NRA and in the ML/TF vertical risk assessment on legal persons and legal arrangements[587].

LBR manages both the RCS and RBE registers, under the authority of the Minister of Justice. LBR is an economic interest grouping whose members are the State of Luxembourg, the Chamber of Commerce (*Chambre de Commerce*) and the Chamber of Skilled Trades and Crafts (*Chambre des Métiers).*[588]. LBR conducts data validation checks on the registers' information, primarily upon receipt of new information (whether from new companies registering, or updates on existing companies' information). LBR can also refer cases to the prosecution authorities in case it detects companies with severe deficiencies in their filing obligations[589]. Such activities are relevant, as they constitute indirect mitigating factors to preserve the integrity of register data. While the scope of these activities was in the past relatively limited, LBR has since 2021 been undergoing an important strategic transformation, supported by a review of its legal mandate and missions, which contributes significantly to Luxembourg's AML/CFT framework and the TFS implementation controls in particular, namely:

- LBR is implementing centralised sanctions screening checks on its registers' data, which specifically contributes to Luxembourg's controls for TFS implementation (including for PF and TF);
- The legal missions of LBR and its internal capabilities are being expanded to perform more pro-active and risk-based monitoring activities, which contributes to maintaining data quality and completeness as well as ensuring that data is up to date.

A review of the legal framework around enforcement of filing obligations of entities has been performed in view of providing LBR with (i) (administrative) sanctioning powers to impose fines on entities failing to comply with their legal filing obligations and (ii) a broader role in enabling the administrative dissolution of entities deemed to be inactive, both of which contributing to promote compliance by legal persons and reducing the prevalence of shell companies that may be misused for sanctions evasion purposes, as outlined below:

[586] Website of LBR (link)

[587] Luxembourg, *ML/TF vertical risk assessment on legal persons and legal arrangements*, 2022 (link)

[588] European e-Justice Portal, *Business Registers in EU Countries: Luxembourg*, accessed July 2025 (link)

[589] For example, Luxembourg law provides for a fine of between EUR 1,250 and EUR 1,250,000 for a registered entity which fails to file their beneficial ownership details with the RBE or which files inaccurate, incomplete or out-of-date beneficial ownership details.

(i) Amendments to the RCS and RBE legal framework[590] enhance the oversight and enforcement powers of LBR to ensure that the data collected remains adequate, accurate and up to date. The new powers comprise the following:

(a) to require registered entities to update the information if the ongoing monitoring by LBR reveals that the data are outdated;

(b) to impose administrative sanctions and measures, such as public notices that a verification procedure is launched (to inform all RBE users), certificates of non-compliance and daily penalty payments.

The amendments also foresee an automatic consistency check between the RCS and the RBE on the accuracy of the information.

(ii) A procedure for administrative dissolution without liquidation was set up in 2022[591]. This procedure allows for the dissolution of a company and thus the end of its legal personality without going through the process of a full formal judicial liquidation (as per article 1200-1 of 1915 Companies Law, as amended). The entities that can be subject to this procedure are commercial companies which (i) have no employees, (ii) have no assets and (iii) pursue activities contrary to criminal law or seriously contravene the provisions of the Commercial Code or the laws governing commercial companies (such as lack of a registered office, lack of a manager, failure to file annual accounts, etc). The objective is to dispose of "empty shells", that is companies which no longer have a reason to exist, in a short time and at a lower cost for public authorities. This procedure can be initiated by the State Prosecutor and has been implemented by LBR since June 2023.

As previously mentioned, the fact that all firms in Luxembourg are inherently legal persons or arrangements means that some are already subject to close supervision by their respective supervisors (e.g. insurance entities by the CAA). As such, it is correct to say that certain entities are subject to certain controls by virtue of their sub-sector.

Keeping RCS and RBE data up to date

To keep data up to date, LBR has set up an automated monitoring system for a number of criteria. This enables it, first and foremost, to take proactive measures with registered entities to ensure they keep their data up to date, even before a deadline arrives. Thus, when the renewal date of a mandate or the filing date for annual accounts approaches, for example, LBR will inform the entities concerned so that they can take the necessary steps within the legal deadlines. If the company acts late, i.e. if it takes the necessary steps more than 30 days after the event making its filing mandatory, as provided for by law, it will be subject to an increase in its filing fees.

This monitoring also enables the implementation of administrative measures and sanctions provided for by law[592]. Entities found to be in non-compliance with company law, and more specifically with their filing and publication obligations, will face progressively increasing administrative measures:

- 1st measure: warning on the LBR website, stating that the file is under review
- 2nd measure: notice on the extracts/certificates issued by LBR on which the breaches identified are listed and are visible to all users, directly on the LBR website
- 3rd measure: financial penalty

590 Law of 23 January 2025 (link)
591 Law of 28 October 2022 (link)
592 LBR launched the first preventive phase at the end of January 2026 and is expected to start the second enforcement phase in the second quarter of 2026.

- 4th measure: striking off. After being struck off, the entity appears in the RCS with a "struck off" reference. This status will be visible to all users of the RCS
- 5th measure: transfer the file to public prosecutors for further investigation

Note that the information contained in the RCS is publicly available and that access to the information is free of charge. This enables ex-post control of the information during which third parties can report discrepancies or errors to LBR.

The following table shows the number of legal persons registered with the RCS over recent years.

Table 30: Legal persons registered with the RCS at year-end[593], 2018-2023

	31/12/2018	31/12/2019	31/12/2020	31/12/2021	31/12/2022	31/12/2023
Sociétés commerciales	129,120	132,633	121,918	121,916	126,485	128,265
Sociétés civiles	5,140	5,203	5,478	5,845	6,065	6,068
ASBLs	11,248	11,518	8,504	8,457	8,717	8,806
Fondations	214	217	218	193	192	193
Other legal persons	3,233	3,194	3,096	3,019	3,027	3,041
Total	**148,945**	**152,765**	**139,214**	**139,430**	**144,486**	**146,373**

Enforcement capacity provided by the 1915 Companies Law

Article 15 of the 2002 RCS Law requires a company to file any amendments concerning its basic information (e.g. name, address, proof of formation, etc.) within one month. Article 19-1 of the 2002 RCS Law further states that deeds, extracts thereof and information required to be published by law shall be filed by electronic means with the RCS within one month following the date of the finalised deed. These provisions go hand in hand with article 100-13 of the law of 10 August 1915 on commercial companies (the "1915 Companies Law"). The latter lists what information needs to be lodged with the RCS and published with the RESA. A breach of these obligations could lead to the legal persons' managers being held liable (article 441-9 of the 1915 Companies Law) or to the closure of the company by application of article 1200-1 of the 1915 Companies Law. Article 1200-1, paragraph 1, of the 1915 Companies Law permits the District Court dealing with commercial matters to, at the discretion of the State Prosecutor, order the dissolution and the liquidation of any société commerciale with a separate legal personality governed by Luxembourg law which pursues activities contrary to criminal law or seriously contravenes the provisions of the Commercial Code or the laws governing sociétés commerciales (including those laws governing authorisations for doing business).

It should be noted that the law of 7 August 2023 applicable to fondations and ASBLs and the law of 25 March 1991 on economic interest groups foresee similar provisions as article 1200-1, paragraph 1 of the 1915 Companies Law. This legal procedure leads to the removal from the register of the company in question. In this case, a judicial representative (usually from a regulated profession such as a lawyer, chartered professional accountant or (approved) statutory auditor), called a "liquidator", is appointed by the court. The mission of this judicial representative is to identify, recover (i.e. collect sums owed to the company) and sell assets of the dissolved company. The generated funds are then used to pay off the company's debts, pay the cost of liquidation and, if applicable, distribute any remaining funds (a "liquidation bonus") to the

[593] Data provided by LBR and from Luxembourg, *ML/TF Vertical Risk Assessment Legal Persons and Legal Arrangements*, 2022

partners/shareholders. If the partners/shareholders of the company have not been identified, the liquidation bonus is paid to the Consignment Office (the State Treasury and more precisely the Caisse de consignation being the official depositary of the Government) and allocated to the Luxembourg State after a retention period of 30 years. The following table shows the number of liquidations that have been pronounced each year between 2015 and 2020:

Table 31: Number of judicial liquidations[594], 2015-2023

Year	Number of judicial liquidations
2015	526
2016	513
2017	488
2018	546
2019	568
2020	942
2021	1,032
2022	859
2023	543

Other enforcement capacities available under the 1915 Companies Law

In relation to updating the relevant shareholder registers, the 1915 Companies Law provides for criminal liability under article 1500-12, which states that managers or directors are punishable by a fine of between €5,000 and €125,000 if they knowingly:

- fail to keep a register of registered shares in accordance with the law;
- fail to appoint a depositary or do not deposit bearer shares with a depositary;
- acknowledge the rights attached to bearer shares in breach of article 430-6, paragraph 5, i.e. failure to deposit bearer shares with a custodian and failure to record mandatory information listed in article 430-6(3) in the bearer share register.

[594] Luxembourg, *ML/TF Vertical Risk Assessment Legal Persons and Legal Arrangements*, 2022 (link) and data provided by LBR.

6.6. Judiciary authorities and law enforcement agencies

6.6.1. CRF

<table>
<tr><th>Stakeholder</th><th>Key responsibilities related to TFS for PF and TF</th></tr>
<tr><td colspan="2">Judiciary authorities and law enforcement agencies</td></tr>
<tr><td>Financial Intelligence Unit (FIU)/Cellule de Renseignement Financier (CRF)</td><td>
• The 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 money laundering (ML), associated predicate offences or terrorist financing (TF).
• In particular, it receives and analyses:
- Suspicious transaction and activity reports transmitted by a professional subject to the AML/CFT legislation as provided by article 5, paragraph 1, a) of the 2004 AML/CFT Law; and
- Information communicated by other AML/CFT competent authorities pursuant to article 74-2 (4) of the amended law of 7 March 1980 on the judiciary organisation.
• The CRF disseminates, spontaneously and upon request, the results of its analysis and any other relevant information when there are reasonable grounds to suspect money laundering, 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.
• 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.
</td></tr>
</table>

The *Cellule de Renseignement Financier* (CRF) is Luxembourg’s Financial Intelligence Unit (FIU). The 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 money laundering, associated predicate offences or TF. In addition thereto, the CRF also proceeds to strategic analysis which focuses on identifying ML/TF related typologies, trends and patterns (1) in order to gain an in-depth understanding of the ML/TF risks, threats and vulnerabilities faced by Luxembourg and (2) to share the strategic intelligence gathered with relevant parties at national and international level.

Prior to the enactment of the law of December 12, 2025 amending the Penal Code and the Code of Criminal Procedure (“Law of December 12, 2025”), article 506-1 of the Criminal Code listed the associated predicate offences that may have given rise to a money laundering offence. In July 2022, failure to comply with restrictive measures as provided for by article 10 of the Law of 19 December 2020 was expressly included in the list of associated predicate offenses of article 506-1 of the Criminal Code. Whilst this new associated predicate offense has broadened the CRF’s competence by extending it to any compliance issues with the Law of 19 December 2020, the CRF was and remained competent for any suspicions in relation to the remaining associated predicate offenses listed in article 506-1 of the Criminal Code. It should be noted that the Law of December 12, 2025 introduced changes to Article 506-1 of the Criminal Code. This amendment removed the approach of maintaining a list of associated predicate offences and extended the offence of money laundering to the proceeds of all crimes and misdemeanors (“*crimes et délits*”). Therefore, when there are suspicions of money laundering or terrorist financing, an associated predicate offense (which may include sanctions lists hits not covered by the Law of 19 December 2020) or a failure to comply with restrictive measures as provided for by article 10 of the Law of 19 December 2020, a report must be filed with the CRF.

However, the sole designation on a sanctions list is not in itself a suspicion of money laundering, associated predicate offense or terrorist financing. Such a designation, respectively any suspicions regarding a failure to comply with restrictive measures as provided for by article 10 of the Law of 19 December 2020, should be considered as an indicator of ML/TF and should trigger a careful review of all the circumstances and factors of the business relationship.

On a related note, articles 59 and 60 of the law of 27 June 2018 regarding export controls specifies several acts of non-compliance with the legal requirements which shall be punished by a prison sentence of 5 to 10 years. These acts may thus also constitute an associated predicate offence to money laundering in accordance with article 506-1 of the Criminal Code, which considers as associated predicate offences to money laundering any crime and misdemeanor (“*crimes et délits*”).

The CRF proceeds to the analysis of the information received in view of possible money laundering, associated predicate offense (including failure to comply with restrictive measures) or TF.

While a designation on an applicable sanctions list in Luxembourg entails an automatic freeze without delay of the concerned person/entity/group’s assets under the responsibility of the obliged entity/person, the CRF’s freeze orders are not automatic, but are taken on a case-by-case basis only, after careful consideration and analysis of each particular situation.

Usually, the reporting entities inform the CRF if the information has already been shared with the MoF; if not, the CRF may urge the reporting entity to enter immediately in contact with the MoF. The CRF and the MoF entered into a Memorandum of Understanding (MoU) on 18 June 2020 in order to strengthen the exchange of information. Such MoU has been amended on 8 February 2022 in order to *expressis verbis* include PF.

That said, often individuals or entities subject to a prohibition or restrictive measure will try to use evasion techniques that include illicit activity and hence may also generate a suspicion that must be reported to the CRF pursuant to Article 5(1)a) of the 2004 AML/CFT Law. In this case, the CRF would receive STRs/SARs based on the illicit activity or transaction suspicion, which may include sanctions indicators. The CRF also receives reports for TF matters in general as part of its competencies (whether or not connected to a sanctions evasion case).

Some reports submitted to the CRF are simple sanctions list matches or homonyms, which are simultaneously reported to the MoF. In instances where it is not obvious based on the report, the CRF will as mentioned above confirm with the reporting entities that they have also reported to the MoF. The CRF not only receives reports based on sanctions lists applicable in Luxembourg, such as UN and EU sanctions lists, but also on lists drawn up by foreign jurisdictions that may not be fully applicable in Luxembourg (such as US/OFAC lists).

It can be highlighted that professionals consider sanctions lists hits as an indicator among others during the onboarding process, in their ongoing costumer due diligence or in their activity/transaction monitoring that triggers further questioning and analysis by that professional. In case of suspicions raised with regard to ML/TF, associated predicate offense or failure to comply with restrictive measures as provided for by article 10 of the Financial Sanctions Law, the professionals file a report to the CRF.

Whenever there is the slightest possibility that a person reported to the CRF is indeed on a sanctions list or a homonym, the CRF sends a request for information to the relevant FIU.

In addition, the CRF conducts strategic analyses to produce reports featuring typologies and indicators designed to raise awareness within the sector and support efforts to detect among others sanctions evasion and PF. The CRF also participates in national and international conferences on these topics, shares intelligence with foreign FIUs, and engages in dedicated international working groups. Furthermore, the CRF is actively involved in strategic public-private partnerships (PPPs) on the topic of circumvention of sanctions.

Freezing orders

In case of suspected money laundering, an associated predicate offense (including failure to comply with restrictive measures) or terrorist financing, the CRF may make use of the freezing power provided for in Article 5(3) of the 2004 AML/CFT Law if such assets do not already fall under an automatic asset freeze. This article empowers the CRF to instruct a reporting entity not to execute transactions in relation to a specific transaction or the client in general. Although the terminology used (i.e. "freezing power" or "freezing order"[595]) is the same as that used for measures taken according to the Law of 19 December 2020, the two measures are completely different.

In practice, the CRF maintains the freezing of funds while allowing national, or foreign judicial authorities by way of a mutual legal assistance request, to order their seizure. The CRF uses its freezing power when sufficient leads suggest that assets held by professionals derive from a criminal activity, thus enabling the competent domestic or foreign authorities to apply for seizure. Pursuant to article 9-3 of the 2004 AML/CFT Law, it is possible to lodge an appeal against the freezing order.

6.6.2. Other judiciary authorities and law enforcement agencies

Stakeholder	Key responsibilities related to TFS for PF and TF
Judiciary authorities and law enforcement agencies	
Prosecution authorities	• Conduct all necessary actions to investigate and prosecute criminal offenses and recover crime-related assets[596]
Investigative judges (*Juges d'instruction*)	• Order measures that restrict individual freedoms (i.e. coercive measures) such as provisional detention, searches and seizures[597]
Judiciary police (*Service de Police Judiciaire*, SPJ)	• Carry out "research and investigations in relation to more serious offenses or of particular complexity"[598], including economic and financial crime

Appearing on a sanctions list is not itself a criminal act, and therefore having assets frozen is understood predominantly as a policy tool. To date, there have been no prosecutions in Luxembourg related to TFS for TF or PF.

However, both ML and TF are criminalised in Luxembourg, with the definition of offences and penalties having been expanded in recent years. Prosecution for ML does require the demonstration, at least in an

595 Pursuant to Article 5 (3) of the 2004 AML/CFT Law, "freezing order" means the ability of the CRF to give instructions not to carry out the operations relating to the transaction or the customer.

596 Luxembourg, *National Risk Assessment* (page 155), 2020 (link)

597 Luxembourg, *National Risk Assessment* (page 155), 2020 (link)

598 Website of the SPJ, accessed June 2026 (link)

implicit but certain manner, of the existence of the constituent elements of the underlying predicate offence (in particular the criminal origin of the pecuniary advantages as well as the circumstance that the defendant was aware of this criminal origin) but not the prosecution of the predicate offence, and can also be based on predicate offences committed abroad[599].

Thus, there may be instances where frozen assets are involved in broader prosecution activity related to TF (as a predicate offence) or PF (if it involves ML activity as a predicate offence) and so involve prosecution/judicial authorities.

If prosecutions were to occur, they would follow the same processes as for ML and TF, involving cross-agency collaboration that includes relevant prosecution and judicial authorities as well as the MoF and relevant supervisors, as required. Files would be shared directly with the prosecution authorities, specifically the General State Prosecutor, representing the prosecution authorities in person or through his or her deputies before the Court of Cassation and the Court of Appeal. Investigative judges may be engaged if coercive measures are required. Alongside this, the judicial police would execute 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[600].

599 Luxembourg, *National Risk Assessment* (page 154), 2020 (link)
600 Luxembourg, *National Risk Assessment* (page 155), 2020 (link)

7. Residual Risk Assessment

The residual risk score is used to identify areas where Luxembourg remains exposed to the highest level of PF/TF sanctions-related risk. It thus serves as a basis to develop and prioritise strategic actions.

Table 32: Consolidated residual risk assessments

Sector	Inherent risk	Residual risk	Sub-sectors[601]	Inherent risk	Residual risk
Banks	**Medium**	**Low**	Retail & business banks (including entities operating online)	**Medium**	**Low**
			Wholesale, corporate & investment banks	**High**	**Medium**
			Private banking	**Medium**	**Low**
			Custodians and sub-custodians (including CSDs)	**Medium**	**Low**
Investment sector – collective investments	**Medium**	**Low**	Collective investments	**Medium**	**Low**
Investment sector – wealth managers	**Medium**	**Low**	Wealth managers (*gérants de fortune*)	**Medium**	**Low**
Investment sector – other			*Brokers dealers*		
			Traders/market makers		
			Regulated securitisation vehicles		
			CSSF supervised pension funds		
MVTS	**Medium**	**Low**	Payment institutions (PIs)	**Medium**	**Low**
			E-money institutions (EMIs)	**Medium**	**Low**
			Agents and e-money distributors acting on behalf of PIs/EMIs established in another EU Member State	**Medium**	**Low**
VAPSs	**Medium**	**Low**	Virtual asset service providers	**Medium**	**Low**
Specialised PFSs	**Medium**	**Low**	Specialised PFSs providing corporate services	**Medium**	**Low**
			Professional depositories		
Support PFSs & other specialised PFSs			*Support PFSs*		
			Other Specialised PFSs		

[601] Sub-sectors indicated in italics were not subject to a deep-dive.

<table>
<tr><th>Sector</th><th>Inherent risk</th><th>Residual risk</th><th>Sub-sectors[601]</th><th>Inherent risk</th><th>Residual risk</th></tr>
<tr><td>Market operators</td><td></td><td></td><td>Market operators</td><td></td><td></td></tr>
<tr><td rowspan="7">Insurance</td><td rowspan="7">Medium</td><td rowspan="7">Low</td><td>Life insurers</td><td></td><td></td></tr>
<tr><td>Non-life insurers</td><td>Medium</td><td>Low</td></tr>
<tr><td>Reinsurance</td><td>Medium</td><td>Low</td></tr>
<tr><td>Intermediaries</td><td></td><td></td></tr>
<tr><td>PSA</td><td></td><td></td></tr>
<tr><td>CAA-supervised pension funds</td><td></td><td></td></tr>
<tr><td rowspan="8">Legal professions, chartered accountants, statutory auditors, and accountants</td><td rowspan="8">High</td><td rowspan="8">Medium</td><td>Lawyers</td><td>Medium</td><td>Low</td></tr>
<tr><td>Notaries</td><td>High</td><td>Medium</td></tr>
<tr><td>Bailiffs</td><td></td><td></td></tr>
<tr><td>(Approved) statutory auditors and (approved) audit firms (réviseurs d'entreprises (agréés) and cabinets de révision (agréés))</td><td>Medium</td><td>Low</td></tr>
<tr><td>Chartered professional accountants (experts-comptables)</td><td>High</td><td>Medium</td></tr>
<tr><td>Accountants</td><td>High</td><td>Medium</td></tr>
<tr><td>TCSPs – professional directors</td><td>High</td><td>Medium</td></tr>
<tr><td>TCSPs – business offices</td><td>High</td><td>Medium</td></tr>
<tr><td rowspan="4">Dealers in high value goods</td><td rowspan="4">Medium</td><td rowspan="4">Medium</td><td>Precious metals, jewelers and clocks</td><td>Medium</td><td>Low</td></tr>
<tr><td>Car dealers</td><td>High</td><td>Medium</td></tr>
<tr><td>Art/antiques</td><td>Medium</td><td>Medium</td></tr>
<tr><td>Luxury goods</td><td>Medium</td><td>Medium</td></tr>
<tr><td>Freeport</td><td>Medium</td><td>Low</td><td>Freeport operators</td><td>Medium</td><td>Low</td></tr>
<tr><td rowspan="5">Legal persons and legal arrangements</td><td rowspan="5">Very High</td><td rowspan="5">Very High</td><td>Sociétés commerciales</td><td>Very High</td><td>High</td></tr>
<tr><td>Domestic "fiducies"</td><td>Very High</td><td>Very High</td></tr>
<tr><td>Foreign trusts</td><td>Very High</td><td>Very High</td></tr>
<tr><td>Associations sans but lucratif (ASBLs) and fondations falling under FATF NPO definition engaged in activities abroad</td><td>Very High</td><td>Very High</td></tr>
<tr><td>Sociétés civiles</td><td></td><td></td></tr>
</table>

Sector	Inherent risk	Residual risk	Sub-sectors[601]	Inherent risk	Residual risk
			Associations sans but lucratif (ASBLs) and *fondations* falling under FATF NPO definition with local activities		
			Other legal entities		

Appendix A. Summary of figures and tables

Summary of figures

Summary of tables

Appendix B. Glossary of key terms and acronyms

Term	Definition
ABBL	Association des Banques et Banquiers, Luxembourg
ADA	Administration des Douanes et Accises
AED	Administration de l'Enregistrement, des Domaines et de la TVA
AIF	Alternative investment fund
AIFM	Alternative investment fund manager
ALCO	Association of Luxembourg Compliance Officers
ALFI	Association of the Luxembourg Fund Industry
ALJB	Association Luxembourgeoise des Juristes de Droit Bancaire
AML	Anti-money laundering
ASBL	Association sans but lucratif
ATM	Automated teller machine
AuM	Assets under management
BCL	Banque Centrale du Luxembourg
BO	Beneficial owner, beneficial ownership
CAA	Commissariat aux Assurances
CDD	Customer due diligence
CdN	Chambre des Notaires
CdH	Chambre des Huissiers
CFT	Combatting the financing of terrorism
CHS	Content hosting services
CPA	Chartered professional accountant
CRF	Cellule de Renseignement Financier
CSSF	Commission de Surveillance du Secteur Financier
DNFBP	Designated non-financial professions and businesses
DNGO	Non-governmental organisation for development (referring to NPOs carrying out development projects abroad and accredited as such by MoFA)
DPRK	Democratic People's Republic of Korea
DRC	Democratic Republic of the Congo
EC	European Commission
EDD	Enhanced due diligence
EMI	Electronic money institution
EU	European Union
EUR or €	Euro
FATF	Financial Action Task Force
GTI	Global Terrorism Index
HCPN	Haut-commissariat à la Protection nationale
HOSSPs	Hawalas and other similar service providers
HQ	Headquarters

Term	Definition
In-scope countries	Afghanistan, Central African Republic, Democratic Republic of the Congo, Democratic People's Republic of Korea, Iran, Iraq, Libya, Mali, Myanmar, Somalia, South Sudan, Sudan, Syria, Yemen
IRE	Institut des Réviseurs d'Entreprises
ISIL	Islamic State of Iraq and the Levant
LBR	Luxembourg Business Registers
KYC	Know your customer
MENA	Middle East and North Africa
ML	Money laundering
MoE	Ministry of the 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
MVTS	Money or value transfer services
NPO	Non-profit organisation
NGO	Non-governmental organisation
NRA	National risk assessment
OAD	Ordre des Avocats de Diekirch
OAL	Ordre des Avocats de Luxembourg
OCEIT	Office for Export, Import and Transit Controls (*Office du contrôle des exportations, importations et du transit*)
OEC	Ordre des Experts-Comptables
OECD	Organisation for Economic Cooperation and Development
OFAC	Office of Foreign Assets Control
PE	Private equity
PoE	Panel of Experts
PEP	Politically exposed person
PF	Proliferation financing
PI	Payment institution
RBA	Risk-based approach
RBE	Register of Beneficial Owners (*Registre des Bénéficiaires Effectifs*)
RCS	Trade and Company Register (*Registre de Commerce et des Sociétés*)
RUSI	Royal United Services Institute
SAR	Suspicious activity report
SNRA	Supranational risk assessment
SNS	Social networking services
SRB	Self-regulatory body
STATEC	National institute of statistics and economic studies (*Institut national de la statistique et des études économiques*)
STR	Suspicious transaction report
Supervisory authorities	CSSF, CAA, AED (as defined in article 1(16) of the 2004 AML/CFT Law)
TCSP	Trust and company service provider
TF	Terrorist financing

Term	Definition
TFS	Targeted financial sanctions
UCI	Undertakings for collective investment
UCITS	Undertakings for collective investment in transferable securities
VA	Virtual asset
VASPs	Virtual asset service providers
UBO	Ultimate beneficial owner
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
US, USA	United States of America
USD or $	US dollar

Appendix C. Inherent risk generic scorecard

Dimension	Description	Rationale	Examples of data insights (non-exhaustive)
Substantiating factors			
Market size & structure	Extent to which the size and complexity of the sector in Luxembourg offers scope for the breach, non-implementation or evasion of TFS for TF and PF	Captures the inherent exposure of a sector to sanctions threats – for example, sector fragmentation can pose greater risk, given sanctioned individuals may choose to operate through multiple or smaller firms.	• Number of entities and revenue/turnover/profit/assets/assets under management vs. number of entities exposed to TFS PF/TF risks • Level of concentration (e.g. top 5 entity assets as a % of the market), and % of these exposed to TFS PF/TF risks • Qualitative assessment of sector fragmentation/complexity
Ownership structure	Extent to which the archetypal firm ownership model (e.g. domestic vs. international, owner type) presents risk of the breach, non-implementation or evasion of TFS	Firms that have HQs/BOs in in-scope countries or in countries that are deemed higher risk or with weaker control increases the potential exposure to the breach, non-implementation or evasion of TFS.	• % ownership by foreign BOs (of which from risky countries based on FATF lists) and % ownership by BOs who are residents in / nationals of in-scope countries • % of entities with a foreign parent and/or in a country exposed to TFS TF/PF risks • Complex legal structures also increase likelihood of disguising true beneficial owners and hence increase the risk of potentially involving sanctioned individuals or companies
Products & services	Extent to which the products and services (e.g. their complexity) offered by the sector offers scope for the breach, non-implementation or evasion of TFS related to PF & TF	Certain products and sectors (e.g. trade finance) are inherently higher risk than others; particular services may make it easier to evade sanctions, such as those that enable the formation of front and shell companies, or add complexity to the value chain (in a way that disguises UBO).	• % of products/services classed as high-risk, in particular based on international guidance (e.g. international trade) • Qualitative assessment of the complexity of products/activities enabled by the sector, and resulting TFS TF/PF risk • Qualitative assessment of the extent to which UBO can be determined by products & services • Qualitative assessment of (inherent) degree of difficulty of implementing sanctions checks on products and activities
Geography/ internationality	Extent to which the frequency and nature of cross-border transactions (including to in-scope countries) presents risk of the breach, non-implementation or evasion of TFS	Sectors which have a higher proportion of international business, particularly with in-scope countries, or those with weaker controls have a higher inherent risk. Given the increasingly circuitous/complex nature of PF and TF value chains, any international exposure (not just with in-scope countries) can present risk.	• % of international business (e.g. in client revenue, assets, transactions), in particular business with countries subject to TFS for PF and TF • % of financial flows with in-scope geographies / high-risk geographies • % of financial flows through multiple geographies (e.g. use of offshore accounts)

Dimension	Description	Rationale	Examples of data insights (non-exhaustive)
Clients	Extent of risk posed by clients, and propensity to be linked to locations or persons subject to TFS for PF & TF	Greater volume of clients can increase likelihood of sanctions; some clients (e.g. those from countries with weaker controls regimes) are inherently riskier than others.	• Total number of clients (stock), new customers per year (flow) • Geographical distribution of customers, incl. % customers designated as high risk (e.g. from countries included in sanctions lists) • Number and % of PEPs: domestic vs. foreign (incl. from countries with higher risk for TFS relating to PF and TF)
Distribution channels & engagement model	Extent to which distribution methods presents risk of the breach, non-implementation or evasion of targeted financial sanctions obligations	Includes factors such as the nature of client interaction (e.g. via intermediaries, online) and transparency and traceability of funds' movement. For example, online distribution channels can be more exposed as it can be easier to obfuscate BO/provide fraudulent documentation.	• Type of interaction: % of face-to-face and indirect interactions (e.g. online), use of intermediaries • Qualitative assessment of fund transparency and traceability (e.g. electronic, physical, virtual) • Usage of social media, crowdfunding, virtual assets or other channels flagged as higher risk in international guidance
Corroborating factors			
Sanctions breach, non-implementation or evasion activity observed in Luxembourg	Observed sanctions breach, non-implementation or evasion activity observed in the sector in Luxembourg	Evidence of sanctions breach, non-implementation or evasion highlights its existence in a sector, but also the potential efficacy of its controls, are used to corroborate the result.	• Number of cases identified (e.g. sanctions reports, investigations, convictions, delisting requests) • Relevant case studies and typologies as identified in Luxembourg • Expert knowledge
Threats exposure	Inherent exposure to common typologies of breach/evasion of TFS for PF and TF (as per international guidance and experience)	This captures the degree to which common sanctions breach, non-implementation or evasion techniques are used in this sector. Given the high level of dynamism in sanctions avoidance and need to stay vigilant to emerging risk typologies/threats, this will be used to validate the sectoral factors.	• Qualitative assessment of exposure to common methods of evasion or techniques for PF/TF (e.g. as listed in international guidance (FATF, UN PoE), peer reviews and case studies • Case studies of sanctions breach, non-implementation or evasion
ML and TF vulnerability	Exposure to underlying sector-specific threats of ML and TF	ML risk and TF risk are distinct from PF risk. However, the consistency of some risk factors (e.g. structure & size of sector) makes this a useful "sense check" of the result.	• NRA inherent risk rating and understanding of common risk factors

Appendix D. Mitigating factors generic scorecard

Dimension	Sub-dimension	Potential data points (non-exhaustive)
Market entry controls	Authorisation model	• Licenses/registrations[602] – number of applications received, processed, approved, rejected • Sanctions screening requirements/controls on market entry
	Breaches	• Number of licenses/registrations breaches (with relation to sanctions list) identified/remediated
Understanding of TF/PF risks *(and related obligations)*	Supervisory understanding of TF and PF risks	• Presence of questions related to TFS/PF & TF risk factors in annual RBA questionnaires • Risk assessments (e.g. institutional, sub-sector risk assessments) • Trainings/typology sharing information for supervisors to stay up to date on latest trends in sanctions avoidance • Qualitative assessment of risk factor awareness across supervisors, including latest sanctions evasion techniques, as defined by FATF guidance and/or UN PoE reports
	Regulation & information	• Communication incl. information on sanctions list updates/publications on TFS issues; evidence of this being up to date (e.g. reflecting latest typologies) • Education/guidance for private sector (e.g. publications, trainings, presence of outreach points for guidance, advice on sanctions screening protocols/best practice, specific details/information that is relevant for sub-sector) • Presence of public-private information sharing partnerships [603] to enable understanding of typologies/cooperation & collaboration
Prevention/ Private sector controls	Screening controls in place	• Sanctions screening approach, incl. involvement of third parties, where relevant, management of alerts incl. degree of false positives, continuous improvement mechanisms and integration with CDD/KYC processes • Approach for enhanced scrutiny of high-risk customers and transactions (alerts generated, etc.) • Qualitative assessment of quality of screening processes (incl. data, where possible, on number of false positives, number of matches, etc.); may come from internal audits
	Internal supporting structures	• Formalised policies, procedures and controls, clearly articulating TFS obligations • Member(s) responsible for TFS, at management and team working level
Prevention/ Private sector controls	Screening controls in place	• Sanctions screening approach, incl. involvement of third parties, where relevant, management of alerts incl. degree of false positives, continuous improvement mechanisms and integration with CDD/KYC processes • Approach for enhanced scrutiny of high-risk customers and transactions (alerts generated, etc.) • Qualitative assessment of quality of screening processes (incl. data, where possible, on number of false positives, number of matches, etc.); may come from internal audits
	Enforcement	• Remedial actions imposed by supervisor on the private sector related to inadequate TFS screening procedures • Outcomes of remedial actions (i.e. number of deficiencies remediated) related to TFS

[602] This does not refer to the authorisations granted by the MoF.
[603] As stated in FATF guidance (2017): "*Sharing information is key to promoting financial transparency and protecting the integrity of the financial system by providing financial institutions, and relevant competent authorities the intelligence, analysis and data necessary to prevent and combat ML/TF*".

Dimension	Sub-dimension	Potential data points (non-exhaustive)
Detection, reporting and outcomes	Reporting framework	• Number and quality of sanction screening match reports issued by sector • Speed of reporting sanctions matches to MoF • Number and quality of STRs filed by sector related to TFS for PF and TF (where relevant)
	Asset freezes	• Number of asset freezes and total value driven by sanctions related offences by individuals or firms in sector
	Outcomes	• Outcomes of sanctions matches, e.g. % of unfrozen assets (challenge/delisting) and % of assets that remains frozen • Number of investigations/prosecutions/convictions driven by sanctions-related offences on individuals or firms in sector