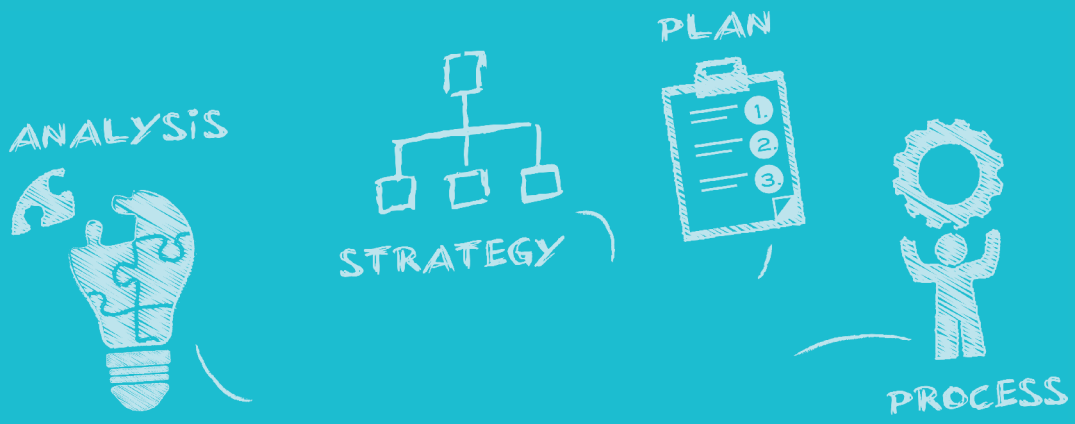
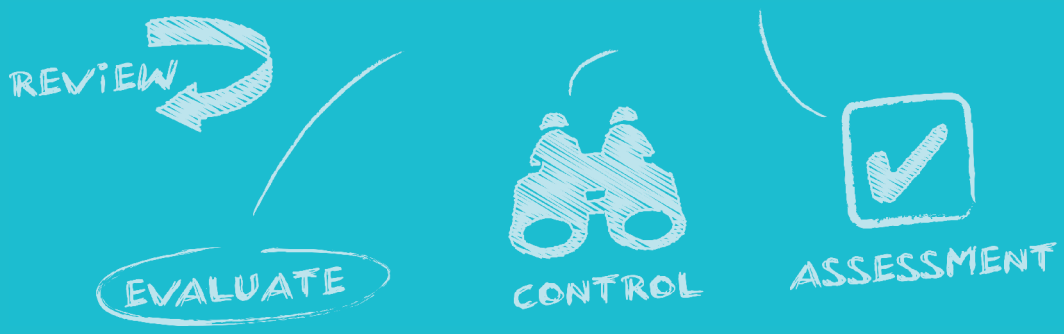


NATIONAL RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING

Luxembourg, 15th September 2020



THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of Justice

1. EXECUTIVE SUMMARY

Money laundering (ML) and terrorist financing (TF) are threats to global security as well as to the integrity of financial systems. The UNODC, IMF and World Bank estimate that laundered proceeds of crime account for 2–5%[1] of global GDP and support several criminal activities. It is estimated that less than 1% of laundered proceeds globally are seized[2,3]. In Europe, it is estimated that only around 2.2% of laundered proceeds are provisionally seized or frozen, and around 1.1% are finally confiscated[4].

Luxembourg has long been committed to fighting ML/TF activities and ensuring that the risks arising from and within its jurisdiction are mitigated. For this purpose, it committed itself to developing a deeper understanding of its specific threats and vulnerabilities through the delivery of a national-level risk assessment ("NRA") in 2018, in the face of growing and evolving ML/TF risks and in line with FATF's recommendations. This report constitutes the latest update of the NRA. It encompasses the latest understanding of Luxembourg's threats, vulnerabilities and the mitigating factors it has taken to reduce the ML/TF risks it faces, including since 2018. Luxembourg intends to use this risk assessment to further advance its risk-based approach to supervision.

In line with a risk-based approach, special consideration is paid to the risks arising from Luxembourg's role as a global financial centre. This role is particularly important in Luxembourg's case, given that the financial sector is the country's largest economic sector (with ~50 900 employees[5] and representing 23% of GDP[6]) with many foreign institutions, foreign-owned assets, and a leading centre for a variety of international financial services businesses in the Eurozone.

1.1. Approach and methodology

The 2020 NRA was led by the Executive Secretariat of the National ML/TF Prevention Committee (NPC), with the input of a wide set of national stakeholders. The exercise was conducted in the first semester 2020[7], and compiles an overview of Luxembourg's current situation as of year-end 2019, using a structured and data-driven approach based on international guidance (e.g. FATF's guidance, the EU's anti-money laundering directives, ESA guidance) and peer practices, and considering Luxembourg specificities where needed.

Throughout the exercise, inputs were collated via a combination of desk-level research, data collection and discussions with the relevant stakeholders for expert input. The research and data collection were conducted across public/private data sources both at the international and national levels. Several different stakeholders, were engaged, consulted and actively involved, as required, to provide input to arrive at an appropriate understanding of risks, including:

- Ministries
  - Ministère de la Justice (MoJ)

[1] See for example: UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011

[2] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011

[3] The UNODC estimates that of the $2.2 trillion in criminal proceeds in 2009, around $1.6 trillion were laundered

[4] See for instance, Europol, *Does crime still pay? – Criminal asset recovery in the EU*, 2016

[5] STATEC, Emploi salarié intérieur par branche d'activité - données désaisonnalisées 1995 – 2019 (4e trimestre 2019) (link)

[6] STATEC, Valeur ajoutée brute aux prix de base par branche (NaceR2) (prix courants) (en millions EUR) 1995 – 2019 (link)

[7] Luxembourg's AML/CFT framework is considered as of year-end 2019, and as such all AML/CFT-related data, legislation, procedures etc. are assessed as of year-end 2019. Nonetheless, some non-AML/CFT-specific data points from first half 2020 are included in this report, as well as some references to draft laws and regulations underway in first half 2020, since this information was available at time of NRA finalisation

  - Ministère des Finances (MoF)
  - Ministère des Affaires étrangères et européennes (MAEE)
- Supervisory authorities
  - Commission de Surveillance du Secteur Financier (CSSF)
  - Commissariat aux Assurances (CAA)
  - Administration de l'Enregistrement et des Domaines et de la TVA (AED)
- Self-regulated bodies (SRBs)
  - Ordre des Experts-Comptables (OEC)
  - Institut des Réviseurs d'Entreprises (IRE)
  - Chambre des Notaires (CdN)
  - Ordre des Avocats de Luxembourg (OAL)
  - Ordre des Avocats de Diekirch (OAD)
  - Chambre des Huissiers (CdH)
- Investigative authorities
  - Cabinets d'instruction de Luxembourg et de Diekirch
  - Service de police judiciaire (SPJ)
- Prosecution authorities
  - Parquet général
  - Parquets près les tribunaux d'arrondissement de Luxembourg et de Diekirch
- FIU
  - Cellule de renseignement financier (CRF)
- Customs
  - Administration des douanes et accises (ADA)

ML/TF NPC meetings held throughout this period helped to review and refine the outcomes of the exercise. The NRA is estimated to have had contributions of more than 15 different agencies, more than 50 specific contributors, 100-plus bilateral discussions, and thousands of data-points and peer practice examples; the report shown here reflects the joint effort across all involved.

In line with FATF's definitions, and as per the first NRA[8], the assessment first understands the level of inherent ML/TF risks in Luxembourg, as a factor of threats[9] and vulnerabilities[10]. Inherent risks stem from Luxembourg's economy, openness, and other structural factors, including its role as a large financial centre. It reflects in part the economic model that has made Luxembourg an attractive country for legitimate businesses. The NRA then assesses the effectiveness of mitigating factors in place, to determine residual risks (i.e. after mitigating factors were considered)[11]. The final step is to

[8] Some methodological refinements were taken to better the assessment since 2018, as described in the methodology section of the report

[9] A threat is a "person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc.", *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment,* February 2013

[10] Vulnerabilities are "those things that can be exploited by the threat or that may support or facilitate its activities", *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment,* February 2013

[11] A classification of risk ranging from "very low" to "very high" is used, reflecting commonly used practices. These ratings should be understood as an assessment of relative risk within Luxembourg. That is, a sector with a "very high" risk is considered more likely to be abused or misused for ML/TF than one with "medium" risk, within Luxembourg

determine the strategic implications for improving the AML/CFT regime in place, by prioritising strategic actions and resource allocations.

1.2. Assessment of inherent risks – threats and vulnerabilities

Luxembourg's threats primarily derive from money laundering of foreign proceeds of crime. The domestic exposure to money laundering (i.e. proceeds from predicate offences perpetrated in Luxembourg available to be laundered) is significantly smaller. The threats of terrorism and terrorist financing are assessed as moderate overall.

The table below summarises Luxembourg's exposure to ML/TF threats, at the level of predicate offences.

Table 1: ML / TF threats[12] assessment (at predicate offence level)

Designated predicate offence	External exposure	Domestic exposure	Overall threat level[13]
Money laundering (average ML threat)	**Very high**	**Medium**	**Very high**
Fraud and forgery	**Very high**	**High**	**Very high**
Tax crimes	**Very high**	**Medium**	**Very high**
Corruption and bribery	**Very high**	**Medium**	**Very high**
Drug trafficking	**High**	**Medium**	**High**
Participation in an organised criminal group & racketeering	**High**	**Medium**	**High**
Sexual exploitation, including sexual exploitation of children	**High**	**Medium**	**High**
Cybercrime	**High**	**Medium**	**High**
Counterfeiting and piracy of products	**High**	**Low**	**High**
Smuggling	**High**	**Low**	**High**
Robbery or theft	**Medium**	**High**	**Medium**
Trafficking in human beings and migrant smuggling	**Medium**	**Medium**	**Medium**
Illicit arms trafficking	**Medium**	**Low**	**Medium**
Insider trading and market manipulation	**Medium**	**Low**	**Medium**
Illicit trafficking in stolen and other goods	**Medium**	**Low**	**Medium**
Extortion	**Low**	**Medium**	**Low**
Environmental crimes	**Low**	**Low**	**Low**
Murder, grievous bodily injury	**Low**	**Very Low**	**Low**
Kidnapping, illegal restraint, and hostage taking	**Low**	**Very Low**	**Low**
Counterfeiting currency	**Low**	**Very Low**	**Low**
Piracy	**Low**	**Very Low**	**Low**

[12] The assessment depicted in this table is based on a mix of research and data available, expert judgement, bilateral meetings and a workshop group discussion with judicial authorities. Exposure to predicate offences constituting the threats was broadly assessed along a set of criteria, namely the probability of the crime occurring, proceeds of the crime if occurring (including size and form of proceeds, and complexity/expertise of ML and geography, where available), and the human, social and reputational impact (the latter for domestic exposure only)

[13] FATF, The World Bank Risk Assessment Methodology, 2017

Designated predicate offence	External exposure	Domestic exposure	Overall threat level[13]
Terrorism and terrorist financing	**Medium**	**Medium**	**Medium**

Luxembourg's threats primarily derive from money laundering of foreign proceeds of crime (i.e. proceeds from predicate offences perpetrated outside of Luxembourg). The magnitude, diversity and openness of financial flows transiting through and managed in Luxembourg contribute to exposure. Indeed, a significant share of requests for mutual legal assistance (MLA) by foreign countries, asset seizures executed in Luxembourg and suspicious transaction reports filed to the country's financial intelligence unit (FIU), relate to possible offences committed abroad. Across all crimes, the prosecution authorities report having received a total of 1 701 MLA requests on aggregate in the past three years of 2017–19, of which 362 are related to self-laundered (SL) ML[14]. Data from Luxembourg prosecution authorities show seizures following MLA requests across all crimes in the past three years (2017–2019) of ~€311.5 million, compared to ~€92.1 million for domestic cases.[15] Luxembourg's FIU and law enforcement agencies have frequent and ongoing cooperation with their foreign counterparts, in particular within the European Union. Most of these foreign offences and proceeds are believed to stem from offences related to fraud and forgery, tax crimes, corruption and bribery and drug trafficking. In fact, these four crimes represent over 70% of estimated criminal proceeds generated globally[16], ~45% of seizures following MLA in 2017–2019[17], and 57% of MLA received in 2017–2019[18]. This is also in line with expert assessment from the country's authorities.

The domestic exposure to money laundering (i.e. proceeds from predicate offences perpetrated in Luxembourg available to be laundered) is significantly smaller. This is due to Luxembourg's low crime rate and limited presence of organised crime. The Organised Crime Portfolio[19] estimates that the aggregate revenue across a set of illicit markets (i.e. drug trafficking, fraud, counterfeiting, theft) in Luxembourg is ~€161 million (~0.4% of GDP), which is close to half the estimate for the EU as a whole (~0.9% of GDP on average). Nonetheless, the country's wealth, economy and central location increase the threat level for certain types of crime, in particular: fraud and forgery, drug trafficking (though mostly street level crime) and robberies or theft.

The COVID-19 crisis has led to unprecedented global challenges and economic disruption. Since the emergence of the virus in December 2019 to the time of writing (July 2020) at least half of the world's population has been impacted by some form of lockdown[20]. In Luxembourg, restrictions were implemented on 12 March 2020[21]. As many economies face significant downturn, financial flows are likely to diminish (indeed, Luxembourg's national statistics bureau has stated it will downgrade short-term prospects for the country)[22]. However, experience from past crises suggests that in many cases illicit finance will continue, and new techniques and channels of laundering money are likely to

[14] Parquet Général Statistical Service, Data received in March 2020; it is estimated that most ML MLA requests are SL-related, however there are also MLA requests that arise from third-party or standalone ML

[15] Parquet Général Statistical Service, data received in March 2020

[16] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011 (link)

[17] Parquet Général Statistical Service, Data received in April 2020

[18] Parquet Général Statistical Service, Data received in July 2018; note that besides requests for LAR received by the prosecution authorities, other Luxembourg authorities (e.g. CRF, Asset Recovery Office, Police) also receive other "foreign requests" for cooperation and/or information sharing.

[19] Organised Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

[20] See, for instance Euronews (link), Business Insider (link)

[21] See gouvernement.lu for further details (link)

[22] STATEC, *Coronavirus threat becomes a reality,* 2020 (link)

emerge[23]. In particular, cybercrime and the risks associated with cyber security have increased since the outbreak of the pandemic and the imposition of lockdown measures driving demand for communication, information and supplies through online channels. Fraud and forgery have also been noted by both domestic and international bodies as a growing threat in the context of the pandemic[24]. The primary fraudulent activities have included: the adaptation of existing telephone or email scams; supply chain fraud, specifically in relation to personal protective equipment (PPE) and other healthcare products; and fraudulent investment scams[25]. A more detailed assessment is provided in the COVID-19 section of the NRA.

The threats of terrorism and terrorist financing are assessed as moderate overall; they are closely connected though terrorist financing is a more likely threat to Luxembourg given its financial centre. Despite no terrorism events in the past and no known terrorist groups in Luxembourg, in view of recent terrorism events in neighbouring countries, Luxembourg raised its level of terrorism threat to 2 (on a scale of 4) in 2015, and has kept it there since[26].

Vulnerabilities arise from sectors that may be exposed to misuse or abuse for ML/TF purposes. The table below summarises the inherent risks by sector in Luxembourg (i.e. before any mitigating factors are applied).

Table 2: Inherent risk assessment (at sector-level)

Category	Sector[27]	Inherent risk level
Financial sector	Banks	High
	Investment sector	High
	Insurance	Medium
	MVTS	High
	Specialised PFSs providing corporate services	High
	Market operators	Low
	Support PFSs & other specialised PFSs	Very Low
Non-financial sector	Legal professions, chartered accountants, auditors, accountants and tax advisors	High
	Gambling	Low
	Real estate	High
	Freeport operators	High
	Dealers in goods	Medium
Legal entities and arrangements		High

[23] EBA, *Statement on actions to mitigate financial crime risks in the COVID-19 pandemic*, 2020 (link)

[24] See, for instance, CRF, *Typologies COVID-19*, 2020 (link); CSSF, *Circular 20/740*, 2020 (link); EUROPOL, *Pandemic profiteering – How criminals exploit the COVID-19 crisis*, 2020 (link); and FATF, *COVID-19-related Money Laundering and Terrorist Financing* (link)

[25] EUROPOL, *COVID-19: Fraud*, 2020 (link)

[26] The level of terrorism threat was raised after the Paris attacks in November 2015, and kept at this level after the Brussels attacks in March 2016 as per communication by the Ministry of State. Level 2 (medium threat) defines a real yet abstract terrorist threat; it consists of increasing vigilance against an imprecise threat and to implement measures of vigilance, prevention and protection of variable and temporary intensity. See Ministère d'Etat Luxembourg, *Press Announcement on 23/03/2016*, 2016

[27] At the time of writing the NRA (July 2020), the Ministry of Justice is in the process of conducting a vertical risk assessment on virtual assets service providers (VASPs). These entities became obliged entities only in 2020, with CSSF designated as competent authority for their AML/CFT supervision, and therefore they are not included in the table

The banking sector is naturally vulnerable to ML/TF risks due to a variety of drivers such as a large customer base, high transaction speed and a large volume of financial flows. Consisting of 128 banks from 27 different countries[28], banking represents 20% of contribution to the GDP[29], with €823 billion[30] in assets, and approximately 5 million accounts opened in Luxembourg banks), which, pursuant to the general understanding of ML practices world-wide, could potentially facilitate the concealment and layering of proceeds or benefits of predicate offences. Also, criminals laundering money or financing terrorism might attempt to integrate laundered funds into the formal economy by using the financial system. In Luxembourg, **Private banking** is particularly subject to ML risks, with key risk drivers stemming from significant exposure to international clients, high concentration of high net worth clients, and the complexity of some products (e.g. wealth structuring activities). The 2019 Private Banking SSRA identified that for Luxembourg, there are three predicate offences especially relevant to the sub-sector: tax crimes, corruption and bribery, and fraud.

The investment sector in Luxembourg is large and diverse with a variety of entities such as wealth & asset managers, broker-dealers, traders/market makers, undertakings for collective investments in transferable securities (UCITS) management companies, alternative investment fund managers (AIFMs), self or internally-managed undertakings for collective investments (UCIs), pension funds and regulated securitisation vehicles. The detection challenges are not to be underestimated, given high market fragmentation in terms of the number of providers and a high volume of retail and institutional investors. **Collective investments** are particularly vulnerable to be abused or misused for different types of fraudulent practices, including for example Ponzi schemes, confidence or boiler room scams and, use of fictitious or shell companies.

Within the insurance sector, considered as being moderately vulnerable in Luxembourg, the life insurance sub-sector outstands as more vulnerable in view of its large size and fragmentation. As of 2019, there are ~36[31] companies in the AML/CFT scope, five of which have a Luxembourgish owner. Approximately half of revenues are generated by five entities, and the share has remained stable over the past 10 years[32], which suggests the market remains structurally fragmented. Moreover, the life-insurance sector is oriented towards foreign residents, exposing Luxembourg to potential international ML/TF activities and high-risk customers. Other ML/TF risk factors for life insurance include the products offered, high volume of transactions and the usage of intermediary distribution channels.

Globally, **money service businesses** (including e-money and payment institutions) are commonly used by criminals engaging in ML/TF activities, given international payments, the speed and volume of transactions and geographical reach. Luxembourg has significantly large institutions in this sector (despite being a concentrated one, with only 20 entities), processing 1,15 billion outflow transactions worth ~€83 billion; these are however mostly cross-border transactions within the European Union[33].

Legal professions, chartered accountants, auditors, accountants and tax advisors are exposed to significant ML/TF risks, globally and in Luxembourg in view of the Trust & Corporate Services (TCSPs) activities they can provide in addition to their core activities (except bailiffs). Taken together, these professions are large in size and fragmented. They serve a wide range of clients and international business, operating in a large international financial centre, with an open economy and a diverse

[28] Banque Centrale du Luxembourg, *Statistiques : Etablissements de crédit ; „tableau 11.01" and „tableau 11.05"* as of February 2020 (link)
[29] STATEC
[30] CSSF *data*, 2019
[31] CAA *data*, 2020
[32] CAA, *Annual Report*, 2018
[33] CSSF 2019 data

resident and working population. The combination of various factors such as power granted to them due to their legal status, essential activity in accessing financial services (for a sub-set of professionals) and a key role as intermediaries drives the significant risk levels. Their ability (except bailiffs) to perform various activities that are considered as particularly ML/TF high risk by FATF, for example TCSP activities[34] and real estate transactions makes these professionals highly vulnerable to ML/TF.

The real estate and associated construction sectors are typically regarded as high risk globally, which is in line with the risk rating in Luxembourg. They often involve large monetary transactions and offer the ability to conceal the true source of the funds either directly through physical persons or via layering of the transaction involving multiple legal entities. The large number of customers (many of whom will have legitimate activities) could offer a level of anonymity to criminals (who could for instance use physical persons as third parties to obscure the ultimate beneficiary). In Luxembourg, the real estate activities sector contributes 8,1% to the country's gross value added in 2019 with about€4,1 billion euros[35]. Furthermore, the real estate and construction sector is very fragmented with >6 500 enterprises involved in real estate related and construction activities[36] and >50 000 employees[37]. Combined production value exceeded €14 billion in 2019.

Legal entities and arrangements (including non-profits), are also commonly regarded to be highly vulnerable to ML/TF crimes. As the OECD observes "[A]lmost every economic crime involves the misuse of corporate vehicles"[38] since they might help conceal origin of funds and/or allow funds to be moved overseas. This is because movements of large amounts of proceeds between legal entities and arrangements may attract less attention and suspicion than movements between individuals. Also, legal entities and arrangements can help conceal identity of ultimate beneficial owners and make the link to criminality more difficult to establish by using layers of entities in multiple jurisdictions. In Luxembourg, there were 137 444 legal entities in the Trade and Company Register as of June 2020.

Trust and company service providers (TCSPs) are a cross-cutting vulnerability with high inherent risk. Several international and national organisations have highlighted the exposure of TCSPs to ML/TF risk, particularly in being abused or misused to conceal ultimate beneficial ownership of funds, and to legitimise the layering or integration of criminal proceeds within the financial system, through various forms of investments and legal structures. Luxembourg TCSPs are particularly exposed to ML/TF, due to four main factors. First, the fragmented landscape of types of professionals acting as TCSPs, all of which are assessed to be high-risk given these professions' structure, size and ownership (including 13 types of entities, from banks to lawyers, regulated by 8 different supervisors or SRBs). Second, the exposure of Luxembourg's financial centre to business originating from multiple jurisdictions, contributing to significant diversity in financial flows and clients (including a large share of private banking and fund transactions) and increasing complexity to identify beneficial ownership of TCSPs clients, source of funds and understanding the activities they conduct. Third, the presence of many legal entities and arrangements contributing to the inherent risky nature of TCSP activities. Finally, the use of intermediaries/third parties by professionals providing TCSP activities in Luxembourg, and non-face to face transactions, contribute to the inherent vulnerability. The 2020 SSRA on specialised PFSs providing corporate services (TCSP activities) identified that for Luxembourg, there are three predicate offences especially relevant to the sub-sector: fraud and forgery, tax crimes, and corruption and bribery.

[35] STATEC, *E2103, Section 7, Code L*

[36] STATEC, latest data available for 2017

[37] STATEC

[38] See for instance, OECD, *Behind the corporate veil: using corporate entities for illicit purposes,* 2001

As of July 2020, the Ministry of Justice is in the process of conducting a vertical risk assessment on **virtual assets service providers (VASPs)** in close collaboration with the CSSF, the CRF and different Luxembourgish private sector entities. These entities became obliged entities only in 2020 and the CSSF was designated the competent authority for their AML/CFT supervision.

The vulnerability to threats is also high in sectors such as MVTS, because of the volume of the sector and significant amount of cross border transactions involved; **specialised PFSs**, due to their ability to provide TCSP services; **and freeport operators,** because of the high risk nature of their activities and international flows.

Other sectors, such as dealers in goods, market operators, support PFSs and other specialised PFSs and gambling are considered less vulnerable, as they are either limited in size, scope or activity in Luxembourg.

There are specific vulnerabilities that are particularly relevant in the context of COVID-19. These include online financial services and virtual assets (which may create more opportunity for criminals to conceal illicit funds within a greater amount of legitimate payments made online); entities in financial distress (which in turn creates opportunities for them to be exploited by criminals seeking to launder illicit proceeds); and the delivery of government or international financial assistance, particularly through non-profit organisations. A more detailed assessment of the impact of COVID-19 on vulnerabilities is provided in the Emerging Risks section of the NRA.

1.3. Mitigating factors

In recent years, Luxembourg has been strengthening its AML/CFT regime. The mitigating factors section of the NRA looks to identify the impact of AML/CFT controls, which serve to mitigate the inherent risks identified for Luxembourg. Thereafter, key areas are identified, where further mitigation is required. This part of the exercise involves an understanding of the current legal framework in place, the set-up and practices of the main AML/CFT supervisory authorities, and the detection (intelligence-gathering), prosecution and law enforcement activities in practice. A comprehensive framework, including criteria to assess, was agreed to form a view on the current AML/CTF controls in place, across relevant authorities, prosecution authorities and law enforcement agencies, and ensure coherence across topics and stakeholders. The results were compared against best practice guidance and peer practice, to help assess how much they contributed to reduce the inherent risks identified above and identify possible areas for improvement. Despite the merits of the regime in place, some sectors emerge as still having high residual risk, i.e. the mitigating factors in place do not account for complete mitigation. This is largely the case in sectors known to be frequently and persistently exposed to abuse or misuse for ML/TF criminal activities, and hence require increased resource allocation, vigilance and procedures by the authorities, professional bodies and firms. Once identified, specific initiatives will be implemented to reduce residual risk on these areas.

An overview of Luxembourg's current AML/CFT regime is provided below.

The ML/TF NPC plays a central role in setting the strategic direction and coordination of the AML/CFT national strategy. It is also in charge of promoting discussion and inter-ministerial committee meetings with the main national bodies and engaging with international bodies. Within it, the Executive Secretariat, established in 2019 to strengthen AML/CFT strategy and coordination on a national level, leads the NRA exercise and the national strategy.

Private sector and AML/CFT supervisors[39] cover a diverse set of sectors and entities subject to the 2004 AML/CFT Law. The powers and practices of supervisors differ significantly, reflecting the specificities of each industry and the risks identified in each sector / sub-sector, in line with a risk-based approach. In general, however, supervisors are responsible for defining the applicable regulations for their supervised (private sector) entities (in line with national laws and competence of each supervisor), promoting awareness of ML/TF risks and AML/CFT obligations, and ensuring compliance (including sanctioning non-compliance). Broadly there has been a steady increase in the awareness and understanding of AML/CFT matters and the carrying out of inspections (on-site or off-site). Since the last NRA, AML/CFT supervisors have increased the level of specialisation within supervisory teams, increased headcounts in AML/CFT departments (improving coordination levels) and enhanced the level of engagement with the private sector. In 2019, AML/CFT supervisors in aggregate undertook more than 250 on-site inspections (in addition to desk-based reviews/off-site inspections), detected ~300 legal breaches and enforced more than 90 remedial actions (in form of sanctions and other warnings).

The CRF (*Cellule de Renseignement Financier*) is Luxembourg's financial intelligence unit, playing a prominent role in the national AML/CFT framework as the primary intelligence and detection agency. The 2018 CRF Law segregated the magistrates from the prosecution authorities, while clarifying the independence of the CRF and confirming the magistrates' power to self-initiate an analysis. The CRF is also a key counterpart in national coordination efforts, with significant links to international FIU counterparts. It plays an important educational role with other national authorities and SRBs (e.g. CdN, OAL and OAD), and relevant reporting from private-sector entities, exchanging feedback on STRs and supporting in awareness-raising and training sessions. The structure of the CRF has been evolving continuously in the past five years, with increased staff, specialisation, training, powers and analytical capabilities. Since the last NRA, the CRF identified reporting entities not registered with goAML, and coordinated with supervisors where needed, to increase the number of registered entities from 747 to 1 409 in two years. It also raised awareness on STRs targeted at sectors where STRs and/or goAML registration were low, such as for notaries and real estate agents; the number of STRs received per year increased by more than 30% between 2017 and 2019. The CRF has increased its cooperation with AML / CFT supervisors, leading to an increase in STRs received. It also published a number of strategic analyses, typologies and guidances on its website to increase awareness by the public and private sector, since the last NRA. The 2018 CRF annual report included analyses on tax offenses, corruption and embezzlement, and investment sector, terrorist financing and BEC fraud[40]. In 2019, the CRF published an analysis of typologies in terms of false transfers (for example, false invoices, use of hacked e-mails)[41] and in 2020 on COVID-19 typologies[42].

Prosecution and judiciary authorities and law enforcement agencies investigate and prosecute criminal offenses and recover crime-related assets. ML and TF are criminalised in Luxembourg and their definitions have been expanded in recent years (including the offences that constitute predicate offences to ML); as such, the number of ML/TF prosecutions and convictions and their related offences has also been increasing. In 2019, the number of persons convicted for self-laundered ML (i.e. cases where the perpetrator of the underlying offence is also prosecuted for ML) amounted to 361, of which 217 received prison sentences. Most convictions relate to offences on drug trafficking, robbery or

[39] Includes the Commission de Surveillance du Secteur Financier (CSSF), the Commissariat aux Assurances (CAA), the Administration de l'Enregistrement et des Domaines (AED) as well as self-regulatory bodies (SRBs) for certain professions such as lawyers, notaries, chartered professional accountants and statutory auditors. Also in scope are the supervisory framework for gambling, cash controls at borders and some obligations to file information with the central company register (RCS)

[40] Sometimes referred to in the US as "business email compromise"

[41] CRF, *Faux virements - analyse des typologies*, 2019

[42] CRF, *Typologies COVID-19*, 2020

theft, and fraud and forgery. Investigations for this purpose are mandated by either state prosecutors or investigative judges (the latter being able to order coercive measures such as detentions and seizures) and executed with the support from the Judicial Police. However, as in other jurisdictions, the amounts recovered through the judicial system, in particular for domestic cases, remain relatively low when compared with the estimated amounts involved in criminal activities. In the period 2017-2019, ML/TF related seizures totalled ~€105 million for domestic cases, and ~€660 million for foreign cases (i.e. following mutual legal assistance requests received); most of these relate to fraud and forgery, corruption and bribery, illicit goods trafficking, participation in organised crime, and robbery or theft.

Finally, international cooperation is at the centre of many of Luxembourg's AML/CFT activities given its open economy and diverse working population. This is ensured at the level of each AML/CFT supervisory authority, FIU, ARO, judicial authority, prosecution authority (e.g. via membership in relevant international groups as well as information sharing mechanisms) and law enforcement agency. It comprises a full set of formal and informal assistance (MLA, extradition, EAW, FIU cooperation, ARO cooperation, police cooperation, etc.) In 2019, ~580 MLA requests were received by Luxembourg, including some 150 that were self-laundered ML-related.

The mitigating factors in place within and across different sectors (as outlined above) reduce the inherent risk level to a residual risk level. Broadly speaking, mitigating factors are strongest in the financial sector, which has been covered by the EU AML/CFT framework since 1991 and has a good awareness of the risks. The table below summarises the inherent and residual risk levels in Luxembourg across different sectors.

Table 3: Inherent and residual risk assessment (at sector-level)

Category	Sector[43]	Inherent risk level	Residual risk level
Financial sector	Banks	High	Medium
	Investment sector	High	Medium
	Insurance	Medium	Low
	MVTS	High	Medium
	Specialised PFSs	High	Medium
	Market operators	Low	Low
	Support PFSs & other specialised PFSs	Very Low	Very Low
Non-financial sector	Legal professions, chartered accountants, auditors, accountants and tax advisors	High	Medium
	Gambling	Low	Low
	Real estate	High	High
	Dealers in goods	Medium	Medium
	Freeport operators	High	Medium
Legal entities and arrangements		High	High

FATF has set out a range of mitigating actions and AML/CFT responses to the evolving risks impacted by COVID-19 [44] Those most important for Luxembourg include (but are not limited to): coordinate

[43] At the time of writing the NRA, the Ministry of Justice is in the process of conducting a vertical risk assessment on VASPs. These entities became obliged entities only in 2020, with CSSF designated as competent authority for their AML/CFT supervision, and therefore they are not included in the table

[44] FATF, *COVID-19-related Money Laundering and Terrorist Financing* (link)

domestically and continue to cooperate internationally to assess the ongoing impact of COVID-19 on AML/CFT risks; strengthen communication and monitoring of the private sector by engaging on the application of their AML/CFT measures; and continue to encourage a risk-based approach to customer due diligence (CDD) to address practical issues. In addition, supervised entities should continue to strengthen their understanding of the developing risks by engaging directly with authorities and reading relevant publications[45]. It is noted that as the COVID-19 pandemic continues to evolve, additional ML/TF threats and vulnerabilities may emerge – the mitigating actions described above serve also to prepare the country for these dynamic risks.

1.4. Looking ahead

Looking ahead, Luxembourg has designed a comprehensive AML/CFT strategy, with the aim of increasing awareness of, compliance and effectiveness with AML/CFT controls across the country.

While Luxembourg's national AML/CFT framework is already mitigating effectively a significant part of the ML/TF risks the country is exposed to, it can be further strengthened to increase effectiveness. The NPC has therefore developed a national AML/CFT strategy, based on the findings of the National Risk Assessment. The national AML/CFT strategy is defined at three levels:

- *Agency-level action plans*: Each relevant agency has developed its own action plan to further mitigate the ML/TF risks that its regulated sector is exposed to;
- *National action plan*: We aggregated and articulated these individual action plans into a comprehensive, national plan; and
- *National strategic priorities*: The NPC identified four areas of particular strategic relevance to focus on; those are the areas that the NPC has identified as likely to have the greatest impact on further enhancing the effectiveness of the national AML/CFT framework.

The following paragraphs outline the main strategic priorities while the following sections detail the national and agency-level action plans.

Further enhancing the prosecution of ML/TF: The NPC will establishing a working group consisting of the MoJ, the general state prosecutor and state prosecutors to identify opportunities to further enhance Luxembourg's approach to prosecuting ML/TF. Specifically, we will redefine how the findings of NRA should feed into the prosecution policy for ML/TF, assess the opportunity to establish two largely autonomous economic and financial crime sections at the public prosecutor's offices in Luxembourg and Diekirch to deal with these crimes, and increase the level of staffing and expertise.

Further developing the ML/TF investigation capabilities: A working group, consisting of MoJ, MSI, investigative offices and judicial police, will propose an approach to further increase the specialisation of investigative judges and judicial police officers for the investigation of economic and financial crime. This may involve setting up separate teams or sections within the investigative offices and judicial police that are dedicated to these crimes. The working group will also define a recruitment and development strategy for these teams to source and train employees with the skill-sets required to investigate complex ML/TF cases.

Harmonising the supervision of DNFBPs: A dedicated working group consisting of MoJ and MoF will review the options to harmonise and/or centralise the supervisory model for DNFBPs and propose a new model, with the view to increase the independence of supervision of DNFBPs and further harmonise the supervisory practices across professions. **Improving market entry controls of TCSPs:** A

[45] At the time of writing (July 2020), COVID-related guidance has been published and/or distributed by a number of relevant bodies, including but not limited to: FATF; EBA; CRF; EUROPOL; INTERPOL; CSSF; CAA; and AED

working group of MoJ, MoF, MoE and SRBs will make a proposal to define a harmonised authorisation process across TCSP activities and sectors and review the fit and proper requirements.

2. INTRODUCTION

2.1. Purpose and objective of the NRA exercise

Money laundering (ML) and terrorist financing (TF) are threats to global security as well as to the integrity of financial systems. The UNODC, IMF and World Bank estimate that laundered proceeds of crime account for 2-5%[46] of global GDP and support several criminal activities. The UNODC estimates that less than 1% of laundered proceeds globally are seized[47]. In Europe, it is estimated that around 2.2% of laundered proceeds are provisionally seized or frozen, and around 1.1% are finally confiscated[48]. Terrorist financing – which involves the raising and processing of assets to supply terrorists with resources to pursue their activities – is another threat across many countries globally.

Luxembourg has long been committed to fighting ML/TF crimes and ensuring that the threats arising from and within its jurisdiction are mitigated. For this purpose, it committed to developing a deeper understanding of its specific threats and vulnerabilities through the delivery of a national-level risk assessment (NRA) in 2018.

As per FATF recommendation 1, countries should identify, assess and understand money laundering/terrorist financing (ML/TF) risks through a national risk assessment (NRA)[49].The NRA exercise is "an essential part of the implementation and development of a national AML/CFT regime, which includes laws, regulation, enforcement and other measures to mitigate ML/TF risks" [50]. It seeks to assess inherent ML/TF risks in a country and the effectiveness of the supervisory regime on reducing these risks.

This report encompasses the latest understanding of Luxembourg's threats, vulnerabilities, and the mitigating factors it has taken, including those developed since 2018, to reduce its ML/TF risks. Luxembourg intends to use this risk assessment to further advance its risk-based approach to supervision, and reduce crime across the economy. The assessment should provide adequate guidance to public-sector institutions and private-sector entities, enable prioritisation and allocation of resources in line with risks identified and better equip Luxembourg to engage with international institutions in combating ML/TF activities. Furthermore, the purpose of this assessment is also to use the results to inform the national strategy on mitigation of ML/TF risks, addressing any deficiencies in an appropriate and timely manner.

The structure of this report closely follows the process undertaken to conduct the NRA. The introductory section is complemented with an overview of Luxembourg and of stakeholders participating in the exercise. Section 3 describes the methodology applied to the exercise, Sections 4 and 5 provide the outcomes of the inherent risk assessment across threat and vulnerabilities (sectors and sub-sectors) respectively. Section 6 details the findings of the mitigating factors review and its impact on current residual risks, Section 7 summarises the residual risks assessment, and Section 8 outlines the emerging and evolving risks for Luxembourg. A brief overview of the EU SNRA against

[46] UNODC, *Report Estimating Illicit Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes* 2011 (link)

[47] UNODC, *Report Estimating Illicit Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes* 2011 (link); Of the $2.2 trillion in criminal proceeds in 2009, around $1.6 trillion were laundered

[48] Europol, *Does crime still pay? – Criminal asset recovery in the EU*, 2016 (link)

[49] Recommendation 1, *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment*, February 2013 (link)

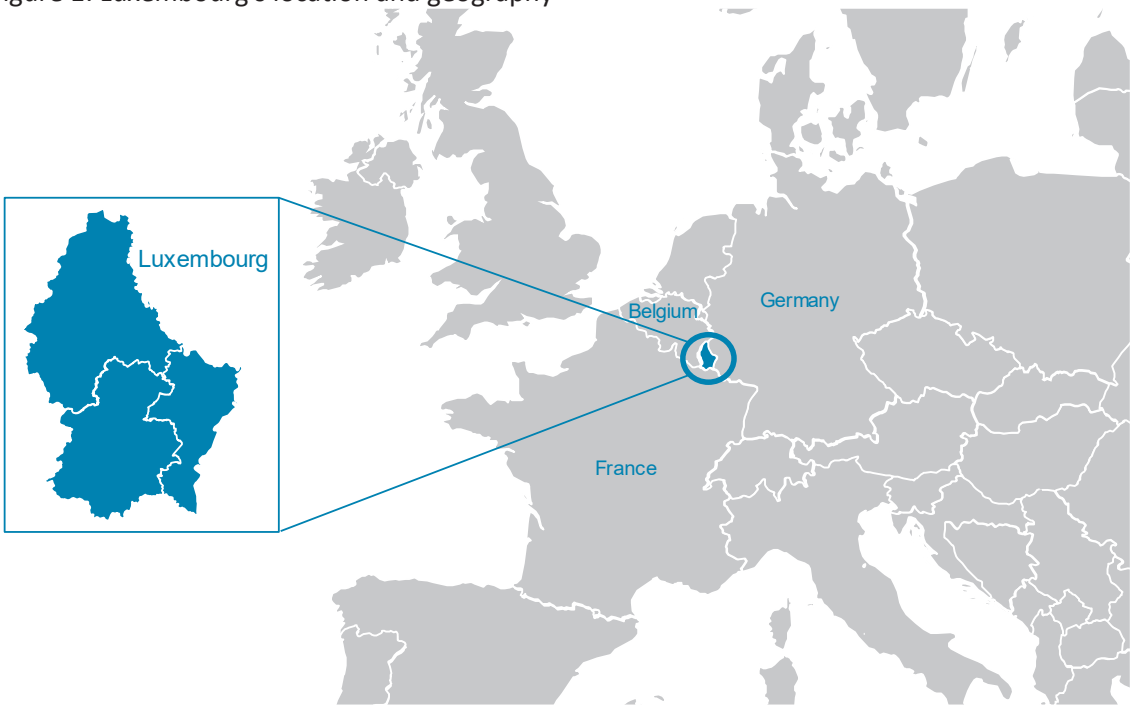
[50] Recommendation 1, *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment*, February 2013 (link)

Luxembourg's NRA in section 9, and a collection of appendices at the end of the report, document additional material that supported the exercise.

2.2. Luxembourg's demographic, economic, legal and political landscape

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

Figure 1: Luxembourg's location and geography



With its total population of 613 900 in January 2019[51], Luxembourg is one of the least populous countries in Europe, but also the one with the highest population growth rate, averaging close to 20% in 2018[52]. The country is relatively densely habited with close to 230 people per km^2. About 47.5% of Luxembourg's population are non-nationals, mostly from Portugal (95 500), France (46 900), Italy (22 500), Belgium (20 000) and Germany (13 000)[53]. Moreover, 44% of Luxembourg's workforce are non-residents living in France, Germany or Belgium and commuting to Luxembourg for work (206 000 out of a total workforce of 465 000 in 2019)[54]. The unemployment rate is low, at 5.5% in January 2020[55]. French, German and Luxembourgish are the three official languages. English is used in certain professional environments, notably in banking and finance.

[51] STATEC, *Population by sex and nationality on 1st January (x 1 000) 1981, 1991, 2001 - 2019* (link)
[52] Eurostat, *Crude rates of population changes*, 2016-18 (link)
[53] STATEC, *Population by sex and nationality on 1st January (x 1 000) 1981, 1991, 2001 - 2019* (link)
[54] STATEC, *Labour market overview (in 1 000 persons) 2000 - 2019*; excludes Luxembourg residents working abroad, civil servants and agents of international institutions (link)
[55] STATEC, *Employment, unemployment and unemployment rate per month (seasonally adjusted) 1995 - 2020* (link)

Luxembourg has been a sovereign and independent state since the Treaty of London was signed on 19 April 1839. Luxembourg is a founding member of the European Union, OECD, United Nations, NATO, UNESCO, the World Trade Organisation, and Benelux Union, reflecting its political consensus in favour of economic, political, and military integration. Luxembourg has always been committed to multilateralism and international cooperation and sees itself as a defender of international agreements and treaties.

Luxembourg City is one of the three "capitals" of the European Union, along with Brussels and Strasbourg. Luxembourg City is home to a number of European institutions, including several departments of the European Commission, the European Court of Auditors, the Court of Justice of the European Union, the European Investment Bank (EIB), the European Investment Fund (EIF), the European Parliament's Secretariat, the European Financial Stability Facility (EFSF), and the European Financial Stabilisation Mechanism (EFSM). The European Public Prosecutor's Office (EPPO) is expected to be operational at the end of 2020 and will have its central office in Luxembourg.[56].

2.2.1. Luxembourg's economy and demographics

Luxembourg's economy is open, dynamic and fast growing with a GDP at market prices of €63.5 billion, thus contributing to about 0.39% of total EU GDP in 2019[57].

Luxembourg has been among the faster-growing economies in the EU with a compounded rate of growth of 2.1% in 2008–2019, compared with 1% for the EU[58]. Year-on-year ("YoY") growth since 2015 has been broadly positive, above YoY growth of EU countries; negative growth was experienced only in three years since 2008, reflecting the recessionary period following the financial crisis as in other European countries.

Table 4: EU28 vs. Luxembourg Real GDP growth (change vs. base year), 2008 - 2019

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	**08-19**
EU28	0.5	-4.3	2.2	1.8	-0.4	0.3	1.7	2.3	2	2.6	2	1.5	**1.0**
Luxembourg	-1.3	-4.4	4.9	2.5	-0.4	3.7	4.3	4.3	4.6	1.8	3.1	2.3	**2.1**

Luxembourg had the highest real GDP per capita among the EU member states in 2019, with ~€83 640 versus an EU average of about €28 650[59]. It should be noted part of this is linked to the high share of non-residents in the domestic workforce (contributing to GDP, but not included in total domestic population figures in GDP per capita)[60].

For most of the 20th century, the steel industry and agriculture were the dominant industries in Luxembourg. The production of raw steel rose from about 145 000 tons in 1900 to 2.45 million tons in 1950 to 6.45 million tons in 1974, with steel representing around 30% of the total value added of the Luxembourg economy and around 16% of the total workforce (with 25 000 people)[61]. From the end of the 1950s, industrial diversification policies and efforts to promote Luxembourg abroad

[56] European Commission, European Public Prosecutor's Office (link)
[57] Eurostat, *GDP at market prices*, 2008-19 (link)
[58] Eurostat, *Real GDP growth rate – volume, Percentage change on previous year*, 2008-19 (link)
[59] Eurostat, *Real GDP per capita*, 2000-19 (link)
[60] Eurostat, *Press Announcement*, 14 December 2017 (link); In terms of Gross National Income "GNI" per capita ($, 2017 in PPP, as reported by the World Bank), Luxembourg also has the highest GNI per capita in the EU with $72 640 vs an EU average of ~$39 000 in 2017 (link)
[61] P. Zahlen, *The Luxembourg economy. An eventful history* (link)

(particularly in the United States) intensified. This was largely the result of the first and second oil crises between 1973 and 1979, which had a significant impact on the Luxembourg economy, in particular the steel industry.[62] The Luxembourg government promoted a policy revolving around three main concepts in the 1960s: a) construction of European and economic cooperation; b) voluntary policy of economic diversification through the implementation of measures to encourage investment; and c) development of an international financial centre. The transformation from an industrial economy dominated by the iron and steel industry to a service economy dominated by financial services was almost accomplished by the mid-1970s.

Today Luxembourg is a leading financial centre[63]. As of the fourth quarter 2019, the financial and insurance sector is Luxembourg's largest economic sector with ~50 873 employees[64] and 25.2% of GDP[65]. As of February 2020, 128 banks were established in Luxembourg; 24 are German, 14 French, 14 Chinese and 13 Swiss[66]. Luxembourg's banking sector today is very large, with banking assets of ~€845 billion, representing ~1 400% of GDP[67]. Moreover, Luxembourg is the leading centre in Europe for investment funds (with ~€4.719 billion net assets under management in Luxembourg funds as of December 2019[68]), the leading centre for private banking in the Eurozone, and the domicile of choice for reinsurance companies.[69] The banks located in Luxembourg specialise in private banking (wealth management for private clients), the functions of custodian bank for investment funds and fund administration, and in the distribution of shares in investment funds. The activities of the financial centre are also diversifying into the fields of microfinance, philanthropy and Islamic finance. Luxembourg for Finance (LFF) is the country's agency for the development and promotion of the financial centre[70].

Besides financial services, Luxembourg has also significantly developed other industries including transport, trade, tourism, telecommunications, e-commerce, broadcasting and business services.[71] Successive Luxembourg governments have pursued pro-active economic development policy, making it possible for Luxembourg to become an international financial centre and establishing itself as a prime business location. For instance:

- **Information & Communication Technologies (ICT)[72]:** Luxembourg is a prime business location for companies from the sector of new technologies and e-commerce, such as Amazon.com, eBay, Skype, Vodafone and PayPal. Luxembourg also hosts SES, created in 1985 in the Luxembourg, the world's leading provider of broadcast and communication services with a fleet of over 50 satellites.
- **Logistics[73]:** 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.

[62] P. Zahlen, *The Luxembourg economy. An eventful history* (link)
[63] See for instance: Z/Yen, Global Financial Centres Index 23, March 2018 (link)
[64] STATEC, Domestic payroll employment by activity - seasonally adjusted data 1995 - 2019 (fourth quarter 2019) (link)
[65] STATEC, Valeur ajoutée brute aux prix de base par branche (NaceR2) (prix courants) (en millions EUR) 1995 – 2019 (link)
[66] Banque Centrale du Luxembourg, *Nombre et origine géographique des établissements de crédit établis au Luxembourg* (link)
[67] Banque Centrale du Luxembourg, *Statistiques : Etablissements de crédit ; „tableau 11.01" and „tableau 11.05"* as of January 2020 (link)
[68] ALFI and CSSF, Net assets under management in Luxembourg funds, December 2019 (link)
[69] The Official portal of the Grand-Duchy of Luxembourg, *The Economy* (link)
[70] Luxembourg for Finance website (link)
[71] The Official portal of the Grand-Duchy of Luxembourg, *Economic Diversification* (link)
[72] The Official portal of the Grand-Duchy of Luxembourg, *ICT* (link)
[73] Luxembourg Trade & Invest, *Logistics Hub Luxembourg*, 2017 (link)

- **Eco-industry:** The Luxembourg hosts about 200 eco-industries working in the fields of renewable sources of energy, waste management, water and eco-construction. They are supported in their work by 28 public-sector agencies and six research institutes. The Luxembourg Eco-innovation Cluster oversees the whole sector.

The table below provides an overview of the evolution of the Luxembourg economy between 1995 and 2017[74]. While the economy has significantly grown over those 22 years, the composition of many sectors has remained relatively constant (e.g. financial services and insurance have always contributed ~25% of gross value added). Science and technology, as well as ICT, have experienced significant growth in both absolute and relative terms since 1995. At the same time, industry/manufacturing has declined in importance.

Table 5: Evolution of Luxembourg economy composition (Gross value added per industry), 1995–2017

	1995	2010	2017
Financial services and insurance	24%	28%	27%
Commerce (incl. reparation of cars and motorcycles)	10%	11%	10%
Science and technology	4%	7%	9%
Real estate	10%	8%	7%
Information Technology & Communication (ICT)	4%	6%	7%
Health and social welfare	4%	5%	6%
General government	6%	6%	6%
Industry/Manufacturing	13%	6%	6%
Construction	6%	5%	6%
Transport and logistics	5%	5%	4%
Education	4%	4%	4%
Administration services and support	2%	3%	4%
Hotels and restaurants	3%	2%	2%
Other sectors	5%	4%	4%
Total gross added value (€ billions)	**14 270 (100%)**	**36 137 (100%)**	**50 276 (100%)**

2.2.2. Luxembourg's political and legal system

Luxembourg is a parliamentary democracy in the form of a constitutional monarchy, with hereditary succession in the Nassau-Weilbourg family[75]; it is the only "Grand-Duchy" in the world. Together with the government[76], the Grand-Duke forms the executive branch in accordance with the Constitution. The Grand-Duke formally appoints a *"formateur"* to form a government that is supported by the parliamentary majority. The government has overall power to manage public affairs and enjoys the right to propose legislation (government bills[77]), and manages the state's income and expenditure budget. The government is based in the city of Luxembourg.

[74] Luxembourg Trade & Invest, *Logistics Hub Luxembourg*, 2017 (link)
[75] The Official portal of the Grand-Duchy of Luxembourg, *Political system* (link)
[76] The Official portal of the Grand-Duchy of Luxembourg, *Government* (link)
[77] The Official portal of the Grand-Duchy of Luxembourg, *Political system* (link)

The legislative power rests on the parliament and the Council of State[78]. The parliament (called Chamber of Deputies) is composed of 60 members and is elected every 5 years by proportional representation in four multi-seat constituencies (south, north, centre, east)[79]. The main function of the parliament is to vote on government bills and parliamentary bills; the Constitution also reserves to the parliament certain powers in financial matters, gives it a right to examine the government's actions, and requires its consent for international treaties to take effect in the country. The Council of State is an independent institution, tasked by the constitution to perform as a moderating second legislative assembly in Luxembourg's unicameral system.[80] The Council of State is composed of 21 State councillors, who are formally appointed and dismissed by the Grand-Duke on proposal by the government, the parliament or the Council of State. The Council of State acts as a consultative organ in the legislative procedure, to ensure compliance with the constitution, international conventions and the rule of law; all bills submitted either by the government or parliament require the opinion of the Council of State.

According to the constitution, the courts and tribunals are responsible for exercising the judicial power, and are independent from the legislative and executive powers. Luxembourg's legal system has its roots in the civil law (continental) family. Luxembourg has a constitutional court (ruling on the constitutionality of laws, excluding those that approve treaties[81]) and three jurisdictions: administrative jurisdictions[82], social security jurisdictions[83] and ordinary courts of law[84]. The administrative jurisdictions are composed of the administrative court and the administrative tribunal, and deal with administrative and fiscal disputes (linked to government administrations, ministries, municipalities and state-owned enterprises).[85] Social security jurisdictions[86] deal with cases where social security claimants take legal action. Ordinary courts of law[87] deal with all other civil, commercial, social and criminal matters and can be divided into:

- **Superior Court of Justice**[88] with authority over the whole territory of Luxembourg. The General State Prosecutor[89] represents the General State Prosecutor's Office[90] at the Superior Court of Justice with authority over the whole territory of Luxembourg.
- **Judiciary tribunals**[91] in the Luxembourg and Diekirch Districts. A state prosecutor represents the prosecution authorities (in each of the 2 "*Parquets d'Arrondissement")*
- **Peace tribunals**[92] in Luxembourg, Diekirch and Esch-sur-Alzette

[78] The Official portal of the Grand-Duchy of Luxembourg, *Political system* (link)
[79] The Official portal of the Grand-Duchy of Luxembourg, *Chamber of Deputies* (link)
[80] The Official portal of the Grand-Duchy of Luxembourg, *Council of State* (link)
[81] Justice Portal Luxembourg, *Cour constitutionnelle* (link)
[82] *Juridictions administratives*
[83] *Juridictions sociales*
[84] *Juridictions judiciaires*
[85] Justice Portal Luxembourg, *Juridictions administratives* (link)
[86] Justice Portal Luxembourg, *Juridictions sociales* (link)
[87] Justice Portal Luxembourg, *Juridictions judiciaires* (link)
[88] *Cour supérieure de justice*
[89] *Procureur Général d'Etat*
[90] *Parquet Général*
[91] *Tribunaux d'Arrondissement*
[92] *Justices de Paix*

3. METHODOLOGY

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

The NRA exercise takes a national perspective (i.e. it is based on the macro-level analysis described in the section "Granularity and scope of the NRA" further below) to contribute to the understanding of ML/TF risks at a country and sector level. It is intended to be in line with FATF's guidance where it states that "*expectations should also be set as to how the results relate to the understanding of national-level risks. Generally, a ML/TF risk assessments is intended to help a country to identify, assess and ultimately understand the ML/TF risks it* faces"[93]. As such, the assessment focuses mostly on supervisory authorities, self-regulatory bodies, the financial intelligence unit, law enforcement agencies and cross-agency committees, where applicable. The methodology also leverages outputs and insights from meso-level and micro-level analyses for collecting more granular inputs and data and enhance the macro-level view.

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

Table 6: Methodology – Key definitions

Term	Definition
Threat (as per FATF[94])	Person or group of people, object or activity with the potential to cause harm to, for example, the state, society and, economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.
Vulnerability (as per FATF)	Those things that can be exploited by the threat or that may support or facilitate its activities. May also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes [*Note "vulnerabilities" are also referred as "sectorial" or "sector" vulnerabilities interchangeably throughout this document*]
Consequence (as per FATF)	Impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally
Risk (as per FATF)	Function of three factors: threat, vulnerability and consequence
Inherent risk	Inherent risk is defined as the risk of ML/TF *before* mitigating actions are applied
Mitigating factor	All elements in place in terms of legal, judicial, supervisory and institutional framework that contributes to combat ML/TF (in one or various sectors) [*note mitigating "factor", "measure", "action" or "framework" are used interchangeably throughout document to refer to this*]
Residual risk	Residual risk is defined as the level of ML/TF risk *after* mitigating measures are applied

[93] FATF, *Guidance on National Money Laundering and Terrorist Financing Risk Assessment,* February 2013

[94] FATF, *Guidance on National Money Laundering and Terrorist Financing Risk Assessment,* February 2013

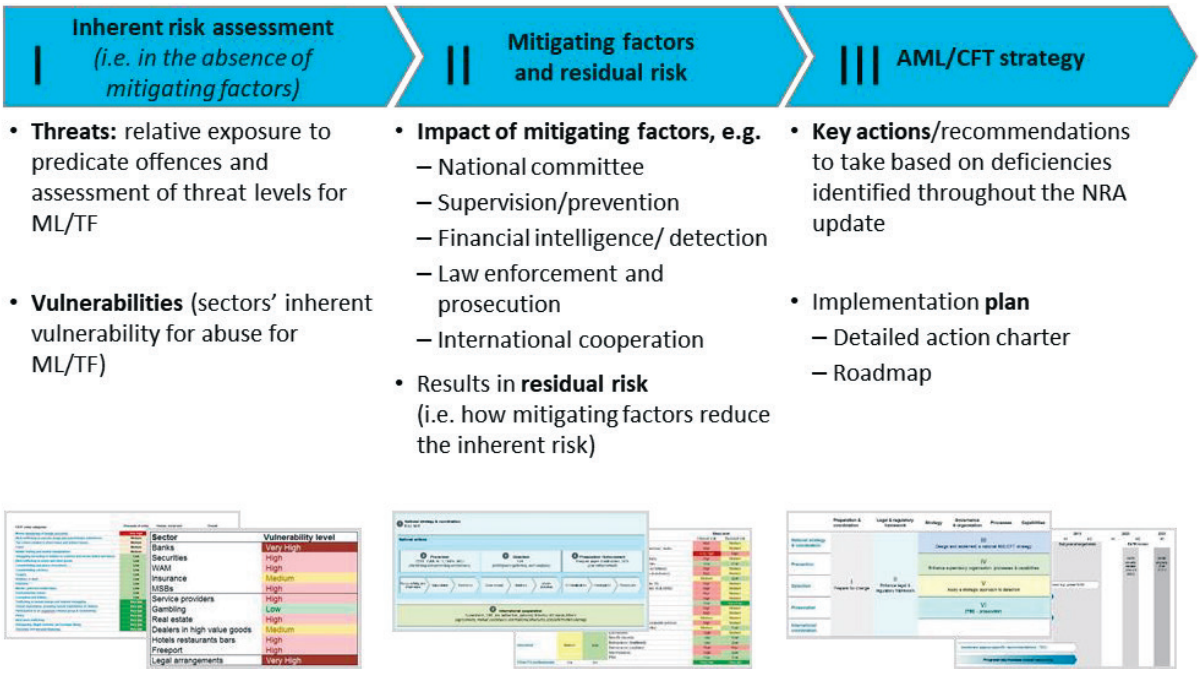
3.1. General approach and process

The NRA exercise is conducted in three steps, from the inherent risk assessment, to the analysis of mitigating factors and residual risk, and finally to the formulation of an updated AML/CFT strategy(as illustrated in the Figure 2 below).

As a first step, the **inherent risk** assessment is performed by analysing threats in Luxembourg (i.e. relative exposure to predicate offences and assessment of threats level to ML/TF), and vulnerabilities (i.e. sectors' inherent vulnerability for abuse for ML/TF). As a second step, mitigating factors and their effects on inherent risk reduction are assessed, resulting in a **residual risk** level.

Finally, the findings of the inherent risk and the impact of mitigating factors as well as the outcomes in residual risks are consolidated and jointly assessed to devise the AML/CFT strategy. The strategy is defined by identifying improvement opportunities of the current set-up that could further increase the effectiveness of the AML/CFT framework. These opportunities for improvement are identified through close collaboration with the different agencies, while taking into consideration guidance from FATF and other institutions and peer practices. Key actions for further improvement are defined based on these opportunities. The AML/CFT Strategy is described in a separate section of the NRA.

Figure 2: Three-step approach of the NRA exercise



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

At all three steps of the NRA exercise, multiple public and private stakeholders were involved. The table below summarises the stakeholders involved in the exercise, grouped by the different dimensions of the mitigating factors framework (further explained in a separate sub-section below).

Table 7: Luxembourg agencies and committees involved in the NRA exercise

Dimension		Stakeholders involved
A	**National strategy & coordination**	• National AML/CFT Prevention Committee (NPC), sub-committees and the Executive Secretariat
B	**Prevention & supervision**	• Supervisory authorities: – Commission de Surveillance du Secteur Financier (CSSF) – Commissariat aux Assurances (CAA) – Administration de l'Enregistrement et des Domaines (AED) • Self-regulatory bodies (SRBs): – Ordre des Experts-Comptables (OEC) – Institut des Réviseurs d'Entreprises (IRE) – Chambre des Notaires (CdN) – Ordre des Avocats de Luxembourg (OAL) – Ordre des Avocats de Diekirch (OAD) – Chambre des Huissiers (CdH) • Agencies performing controls on private sector other than supervisory controls: – Ministry of Justice (MoJ), Ministry of Finance (MOF), Ministry of State (MoS), Ministry of Economy (MoE) – Luxembourg Business Registers (LBR) with regards to the registration of legal entities • Administration des douanes et accises (ADA) as customs administration
C	**Detection**	• Cellule de Renseignement Financier (CRF) • Tax authorities on an ad hoc basis, including Administration des Contributions Directes (ACD)
D	**Investigation and prosecution**	• General State Prosecutor's Office (Parquet Général) • Prosecution authorities (including Parquet de Luxembourg, Parquet de Diekirch, Asset Recovery Office) • Investigative judges • Judicial Police, in particular Service de Police Judiciaire (SPJ)
E	**International cooperation**	• Ministries: Ministry of European and Foreign Affairs (MAEE), MoF, MoJ • Monitoring Committee for International Financial Sanctions

For the inherent risk assessment, different stakeholders were engaged for the threat and the vulnerabilities assessment. For the threat assessment, the analyses were performed together with the prosecution authorities and the CRF, with additional inputs from other agencies (e.g. the CSSF and the ACD). The vulnerabilities assessment primarily involved supervisors and self-regulatory bodies as stakeholders, with additional information collected from other agencies, such as the LBR and the Fiducies and Trust Register (under AED).

The threat and vulnerabilities assessments followed similar stakeholder engagement processes. First, standardised data requests were sent to the supervisors, SRBs and prosecution agencies (including Parquet General, Parquet de Luxembourg and SPJ) to collect relevant data. Bilateral meetings were held with all stakeholders to collect expert insights on the threat or vulnerability status in Luxembourg, identify additional data points to be collected and validate hypotheses on the levels of risk. Following the data and input collection, findings were summarised in an NRA text narrative and scorecards

(further detailed in sub-sections below) and reviewed by the stakeholders via written communication and additional bilateral meetings. This process allowed for increasingly granular analyses, with follow-up communications typically focusing on higher-risk areas.

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

For the AML/CFT strategy formulation, bilateral meetings with relevant stakeholders were held to collect information on the implementation status of the actions from the previous NRA, current and future planned internal initiatives, and to validate hypotheses for improvement identified during the mitigating factors and residual risk discussions. The resulting strategy actions for further improving mitigating factors were summarised and shared via written communication with relevant stakeholders to finalise their scope and timelines.

Given the complexity and large number of stakeholders in the exercise, progress along the three components in Figure 2 above was achieved at a differing pace across agencies and topics. As a result, some authorities were able to complete their assessment ahead of the completion of the exercise and start implementation of agreed improvement measures in parallel with the NRA process. In this case, for the purposes of the NRA, the assessment has been updated to reflect the available data as of the first half of 2020. Similarly, some additional improvement actions identified as needed throughout the 2020 NRA exercise were drafted to be implemented in early 2020. This was deemed adequate and indeed desired, considering one of the key objectives of the exercise was to put in motion measures to address deficiencies as soon as feasible.

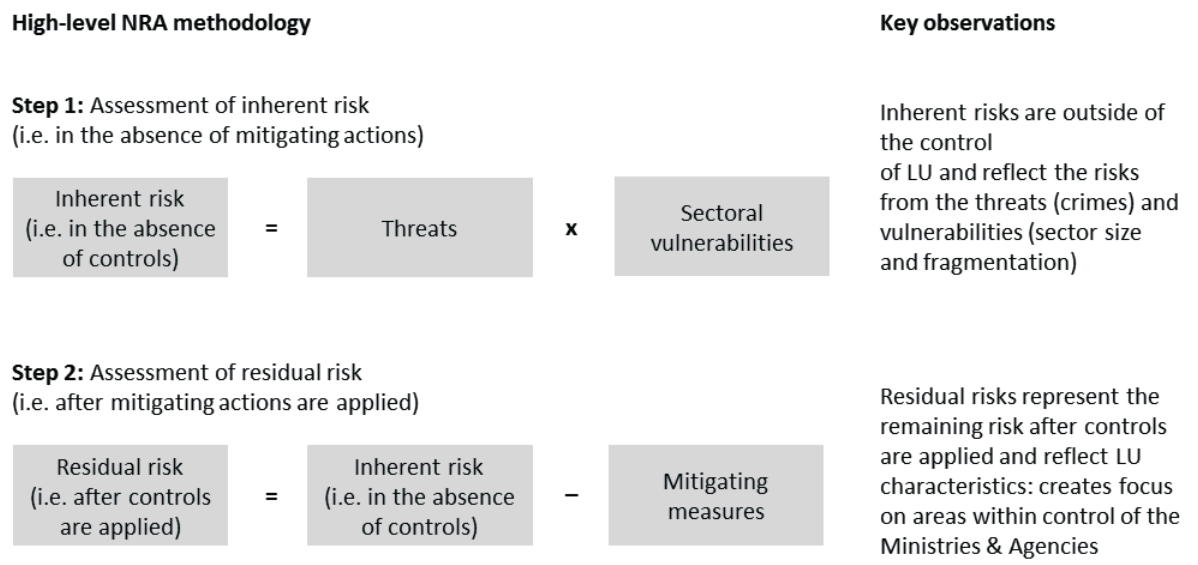
The four sub-sections below describe the two-step approach of inherent and residual risk analysis, define the granularity and scope of the NRA, outline the scorecard approach used and describe data used.

3.1.1. Two-step approach of inherent and residual risk analysis

At a high-level, the approach of this NRA is to assess current ML/TF risks in Luxembourg both before and after considering the mitigating framework in place. The aim is to leverage these results to refine the AML/CFT approach across agencies, and to enable prioritisation of resources across the national supervisors, SRBs, and different prosecution and detection agencies. As introduced in the previous section, the national risk assessment is based on two key steps, illustrated in Figure 3 below:

1. Assessment of inherent risk from threats and vulnerabilities; and
2. Assessment of residual risk once mitigating measures in place are considered.

Figure 3: Overview of inherent and residual risk calculation



Step 1 (inherent risk assessment): ML/TF risks are identified and evaluated for threats (i.e. predicate offences) and vulnerabilities (i.e. sectors most exposed to ML/TF).

Step 2 (mitigating factors and residual risk):

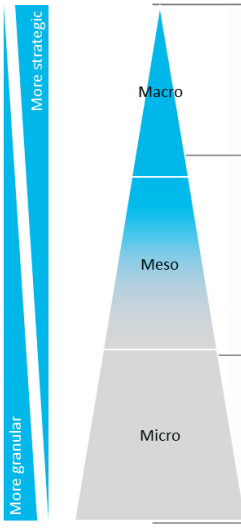
- Mitigating factors: Understanding of Luxembourg's legal, supervisory and law enforcement framework with regards to AML/CFT. The key components of the current framework (i.e. national strategy and coordination, prevention, detection, prosecution and international cooperation) are assessed across four common dimensions: mandate, model, capabilities and results.
- Residual risk: Understanding of how (consolidated) mitigating factors in place reduce the inherent risk computed above (i.e. resultant high-risk areas once mitigating measures in place and their impact is considered).

The second step enables the identification of improvement opportunities in the current mitigating factors framework. The improvement opportunities, identified in close collaboration with the different agencies, are used to define key actions steps which are then consolidated into the AML/CFT strategy.

3.1.2. Granularity and scope of the NRA

Figure 4 (below) illustrates and explains the different levels of granularity of different risk assessment types and links them to the "scope" of the NRA exercise.

Figure 4: Different levels of granularity of risk assessments



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

Part of the NRA exercise

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

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

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

Multiple Luxembourg competent authorities have independently conducted meso-level analyses in the form of sub-sector risk assessments. The published versions of those risk assessments are used as inputs for the NRA: for example, the CSSF's risk assessments on private banking[95] and collective investments funds[96]. The sub-sector risk assessments include granular product or segment taxonomies within an analysed sub-sector, exposure to threats and subsequent vulnerability assessments. The risk assessments also include high-level descriptions of existing mitigating factors put in place both by the public and the private sector.

[95] CSSF, *Sub-sectoral Risk Assessment Private Banking*, 2020

[96] CSSF, *Sub-sectoral Risk Assessment Collective Investments*, 2020

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

This National Risk Assessment focuses primarily on the macro- and meso-analyses insofar as they contribute to the AML/CFT strategy. The micro-analysis is not a focus of this exercise, as this is addressed by the routine supervisory and intelligence analyses. Moreover, the micro-analysis is highly confidential and is for internal use of supervisors, intelligence and/or law enforcement agencies only.

3.1.3. Scorecard approach

The inherent and residual risk assessments leverage a scorecard approach. As such, there is a separate scorecard for the threat assessment, vulnerabilities assessments and the mitigating factors. All scorecards, for the sub-sectors and for the threats, are included in the Appendix of the NRA[97].

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

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

Second, available data and information is collected against each criterion, which is used to form an understanding of the existing levels of threats, vulnerability or mitigation. The collected data and information is transformed into a rating against each criterion, which were formalised in the previous step. During this stage, analyses and findings are drafted into an NRA text narrative.

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

3.1.4. Inputs used

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

Quantitative data from agencies was collected through standardised data requests and through follow-up requests for specific data points. Standardised data requests were sent to different supervisory agencies to collect data on vulnerabilities and mitigating factors and to prosecution authorities to collect data on threats and mitigating factors. Each data point in the data request could

[97] Part of the confidential report, not included in this public version

be mapped against a scorecard criterion for threats, vulnerabilities or mitigating factors. In some cases, additional data was requested from agencies, for example, to further develop the understanding of particular higher-risk factors.

Publicly available quantitative data included both international and domestically available data sets. For example, international datasets from various sources were used, such as international institutions (UNODC, OECD, European Commission, European Central Bank), associations (for instance: BSA Global Software Survey, Global Slavery Index) and academia (including Organised Crime Portfolio). Domestic data sources were used to complete international data sets (e.g. data provided by Parquet Général Statistical Service; CRF Annual Reports; Grand-Ducal Police Annual Reports; STATEC datasets; Banque centrale du Luxembourg datasets; data from LBRs).

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

Expert inputs and judgement of agencies were used to enhance the analyses of threats, vulnerabilities and mitigating factors. For the threats assessment, interviews were used to receive expert inputs on high-risk predicate offences, understand any developments and determine where additional data was needed. Similarly, for the vulnerability assessments, interviews were used to receive inputs on high-risk dimensions of different sub-sectors, understand the sub-sectoral developments over the past two years and identify additional data points to be collected. For the mitigating factors, interviews were used to collect additional information on mitigating factors in place, identify key changes in the mitigating factors over the past two years and key future development areas.

Case studies and typologies were collected from different agencies and public sources to enhance the vulnerability assessment of sub-sectors further. Agencies provided anonymised case studies on previously observed suspicious behaviour by supervised entities or their clients. Typologies from public sources (e.g. MONEYVAL and FATF) were used to illustrate the ML/TF drivers of sub-sectors. The inclusion of case studies and typologies in the NRA is an addition to the previous NRA.

From the data limitations perspective, note that for cases where information was missing, the assessed level of risk has been increased, in line with a conservative approach recommended by the FATF. Note also that in some cases, which represent a minor part of the collected data, the latest available data points were collected for 2018. For example, the number of enforcement measures following on-site visits for 2019 was not final, because some on-site inspections were still being finalised as of June 2020, which could increase the number of enforcement measures for 2019.

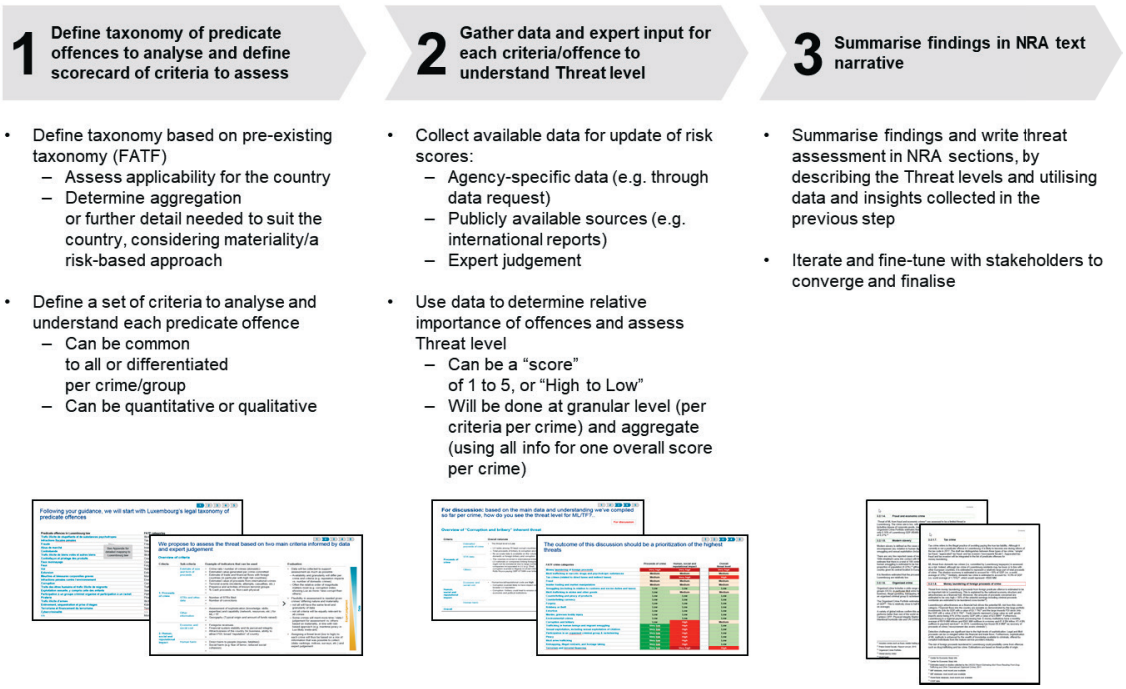
3.2. Methodology for inherent risk

3.2.1. Methodology for threat assessment

The first step of the NRA involves assessing the inherent ML/TF risk (i.e. in the absence of mitigating factors). The approach taken for threats and sectorial vulnerabilities is described below. It should be noted that under threats, ML and TF are assessed separately, given the differing nature of criminal activity. For vulnerabilities, although the purpose and nature of ML and TF may be different, criminals often use similar techniques to move illicit money. Due to the commonality of the methods used, the sectorial vulnerabilities assessment addresses both the exposure to ML and TF without differentiation under its analysis.

The objective of the analysis of threats is to understand the environment in which predicate offences are committed to identify their nature and to assess the exposure to them. The threats assessment is conducted by following the three-step scorecard approach illustrated in Figure 5 (below) by defining the relevant threat taxonomy and agreeing assessment criteria, collecting data and expert input to form an understanding on threat levels, and summarising the final outcomes in a text narrative, iterated and aligned with the relevant experts.

Figure 5: Scorecard approach for threat assessment



In terms of granularity for analysis, threats are assessed along a list of predicate offences in line with FATF crime categories[98]; these map to granular predicate offences (*"infraction primaires"*) under Luxembourg law. Minor adaptations are made to better reflect Luxembourg's reality (for instance, merging "fraud" and "forgery"). The list of predicate offences to ML analysed is provided in Appendix A.2, together with a full mapping table to Luxembourg detailed offences. The exposure to these threats is considered separately for domestic and foreign offences. It should be noted that terrorism and terrorist financing are also predicate offences to ML.

Compared to the previous NRA in 2018, the taxonomy has been expanded to include cybercrime, following its assessment in the 2018 NRA as an emerging and evolving threat. The 2018 NRA assessed cybercrime to be especially important to Luxembourg given its increasing digital economy and prevalence of ICT and fintech companies.

To assess the exposure to these different threats, a scorecard approach was taken. This defined three main criteria (the scorecard is also illustrated in Figure 6, below):

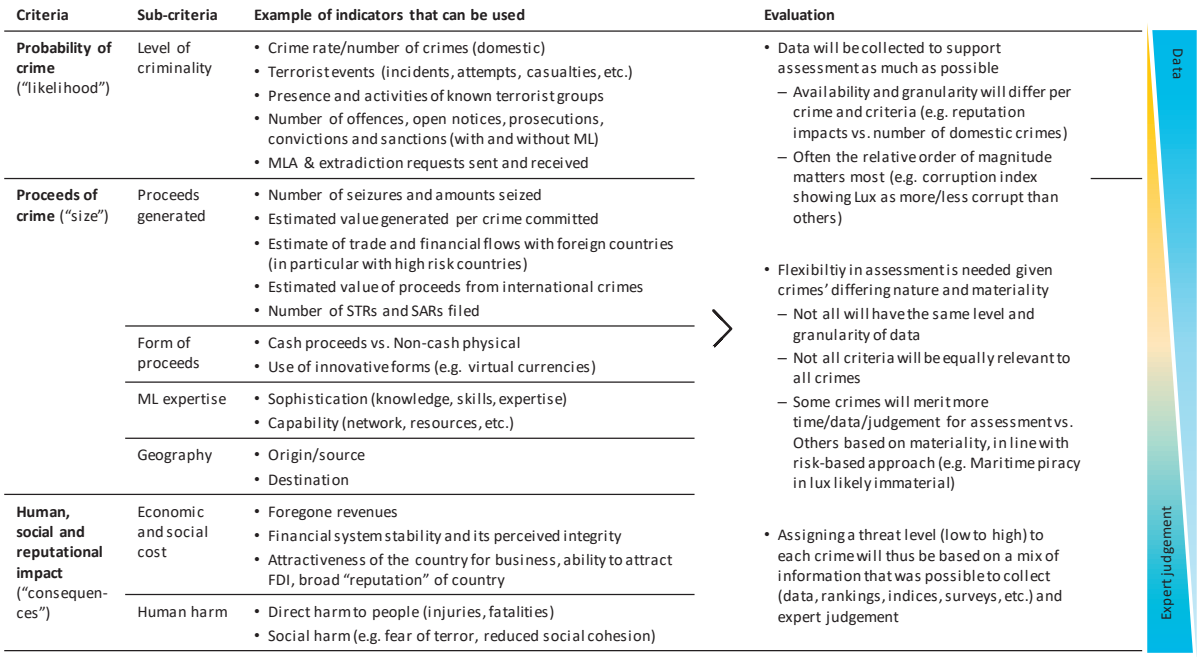
- The "**likelihood**" criterion assesses the level of criminality (e.g. crime rate, terrorist events, presence of terrorist groups, number of offences and convictions).
- The "**size**" criterion assesses an estimate of the proceeds generated (e.g. amounts seized, value generated, number of STRs…) and of the complexity and characteristics of the laundering, i.e. form

[98] FATF NRA Guidance, February 2013, Annex I (link).

of proceeds (e.g. cash versus non-cash), ML expertise of criminals and geography (origin / destination).

- The "**consequences**" criterion helps to distinguish the extent of different threats on financial systems and institutions, as well as the economy and society more generally (i.e. human, social and reputational impact). This is used for domestic, but not foreign offences.

Figure 6: Overview of threat assessment criteria



Threats are assessed on a scale of 1 to 5 (very low, low, medium, high and very high), against the scorecard of criteria using a combination of national and international data available and expert judgement, as well as a workshop with all judicial authorities to validate outcomes.

Threat assessments are done separately for domestic and foreign offences. For instance, a given threat with three scores of "medium" for domestic offences would yield an overall level for the threat domestically of "medium". Following that, the exposure to each threat across domestic and foreign offences is combined for an overall exposure level. It is based on a weighted average between domestic and foreign exposure, with 25% and 75% weights respectively[99]. Given Luxembourg's open economy and large financial sector, the country is more exposed to ML from criminals abroad than domestically. For simplicity, the weighting is assumed to be constant across predicate offences.

The resulting assessment is described in the threats assessment section of this NRA.

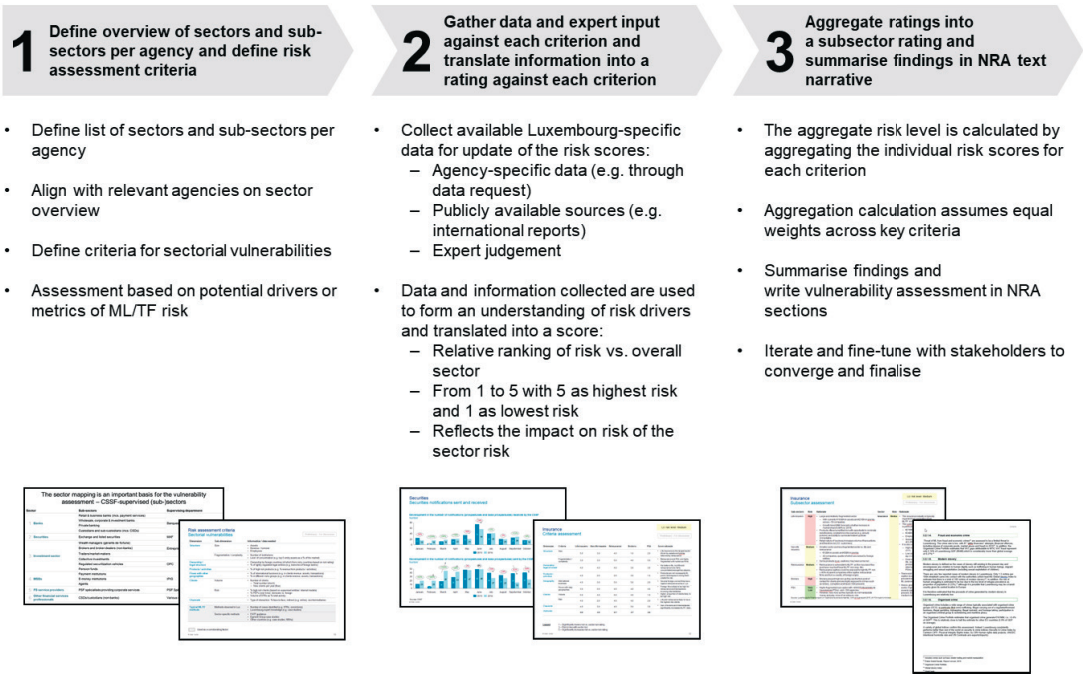
3.2.2. Methodology for vulnerabilities assessment

For the sector/subsector vulnerabilities a similar three-step approach is utilised as for the threat assessment (Figure 7, below). First, an overview of sectors and sub-sectors is defined per agency and

[99] The domestic/foreign weighting was agreed to reflect an average perceived split across offences and sectors, based on expert judgement and data, where available (for instance, share of assets under management outside of Luxembourg in the financial sector).

aligned with each agency. This represents the taxonomy of the sectors and sub-sectors for which the vulnerability will be assessed. In addition, risk assessment criteria are defined for sectorial vulnerabilities, assessing the contribution of each criterion as a potential driver of ML/TF risk. Second, data and inputs are collected from public sources and private sources through data requests and interviews with agencies, which are then matched against the criteria and transformed into ratings, and are used to form an understanding of ML/TF risk drivers for specific sub-sectors. Third and final, ratings are aggregated into a sub-sectoral rating to determine overall inherent risk level, and the analyses are summarised in text narratives, which are presented in the sections below.

Figure 7: Scorecard approach for vulnerability assessment



The methodology used to map the sub-sectors to the sectors is driven by how the supervision of these sectors is organised under the various public-sector supervisory authorities. Therefore, this assessment involves sectors not mapped based on activity but based on supervisory set-up[100]. For instance, the market operators sector in the vulnerabilities assessment only includes the Luxembourg Stock Exchange. Traditional sectors such as fund and asset managers, securities brokers and others are included under the investment sector. The detailed mapping tables for the analysed sectors are included in Appendix A.1.

As described in the three-step scorecard approach to the vulnerability assessment, as part of the first step of the overall approach, the dimension criteria for the risk assessments are specified. The **criteria used in the scorecard** for sectorial vulnerabilities include six dimensions and nine sub-dimensions:

- Structure (consisting of size and fragmentation/complexity)
- Ownership and legal structure
- Products and activities
- Geography (consisting of international business and flows with weak AML/CFT measures geographies)

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

- Client and transactions (consisting of volume and risk)
- Channels

Quantitative data and qualitative information are gathered from national data sources (some public, some confidential) along the dimensions of the assessment criteria. The data and information gathered are then translated into an informed vulnerability rating on a scale of 1 to 5 against each criterion (5 representing highest impact of vulnerability to ML/TF). Where data was missing, expert opinion was used to enrich the analysis. The criteria scorecard for the inherent risk scores, together with examples of indicators and data used can be found in Appendix A.3.

The aggregate inherent risk score across each sub-sector/crime is calculated by averaging the scores against each criterion. Equal weighting was given to each criterion. The aggregate inherent risk score is then mapped to one of the five outcome levels, ranging from “very low” to “very high”. The risk level outcomes are specified in the Appendix A.3. A separate vulnerability inherent risk outcome is been assigned to each sub-sector following the scorecard approach described above. The outcomes of the sub-sector analyses are then aggregated into sectoral outcomes by consolidating them together.

As seen in the sectorial vulnerabilities section below, each sub-sector has a risk level associated with it, which may be different from that of the aggregate sector. Aggregation of scores allows determination of relative risk of sub-sectors within a sector (e.g. life insurance is riskier than non-life insurance in the insurance sector).

3.3. Methodology for mitigating factors and residual risk

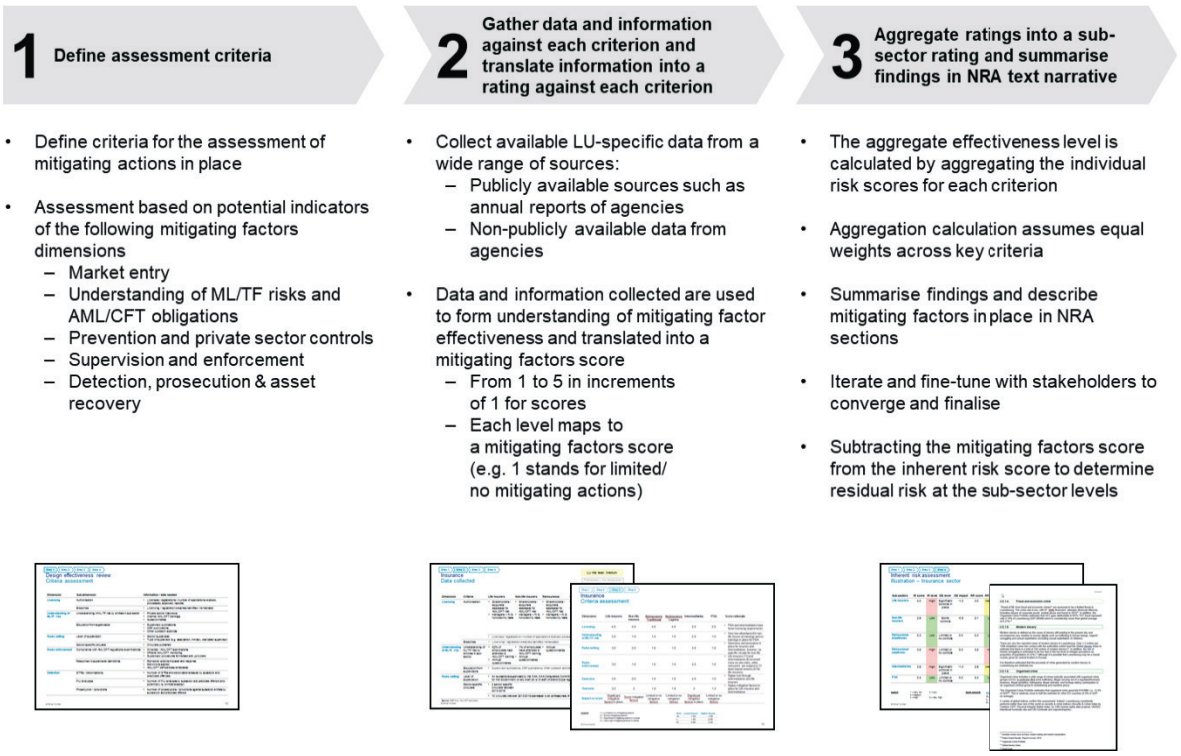
3.3.1. Methodology for impact of mitigating factors

Following the inherent risk assessment, impact of mitigating factors is assessed. An effective system is one that “correctly identifies, assesses and understands its money laundering and terrorist financing risks, and co-ordinates domestically to put in place actions to mitigate these risks”[101]. The aim of this part of the NRA is to establish an accurate, factual picture of the current AML/CFT framework and set up of relevant institutions, and identify improvement measures.

The approach to assess the impact of mitigating factors is structured around three key steps, illustrated in Figure 8, below. First, criteria to assess impact of mitigating factors in place are defined: Those include prevention, supervision, detection and other appropriate mitigating factors levers. As a second step, data and information are collected against each criterion to form an understanding of the effectiveness of the mitigating factors, and each criterion is assigned a score. Finally, the mitigating factors put in place are described in separate NRA sections, and the mitigating factors scores are aggregated for each sub-sector. The aggregated scores are then used to evaluate residual risk.

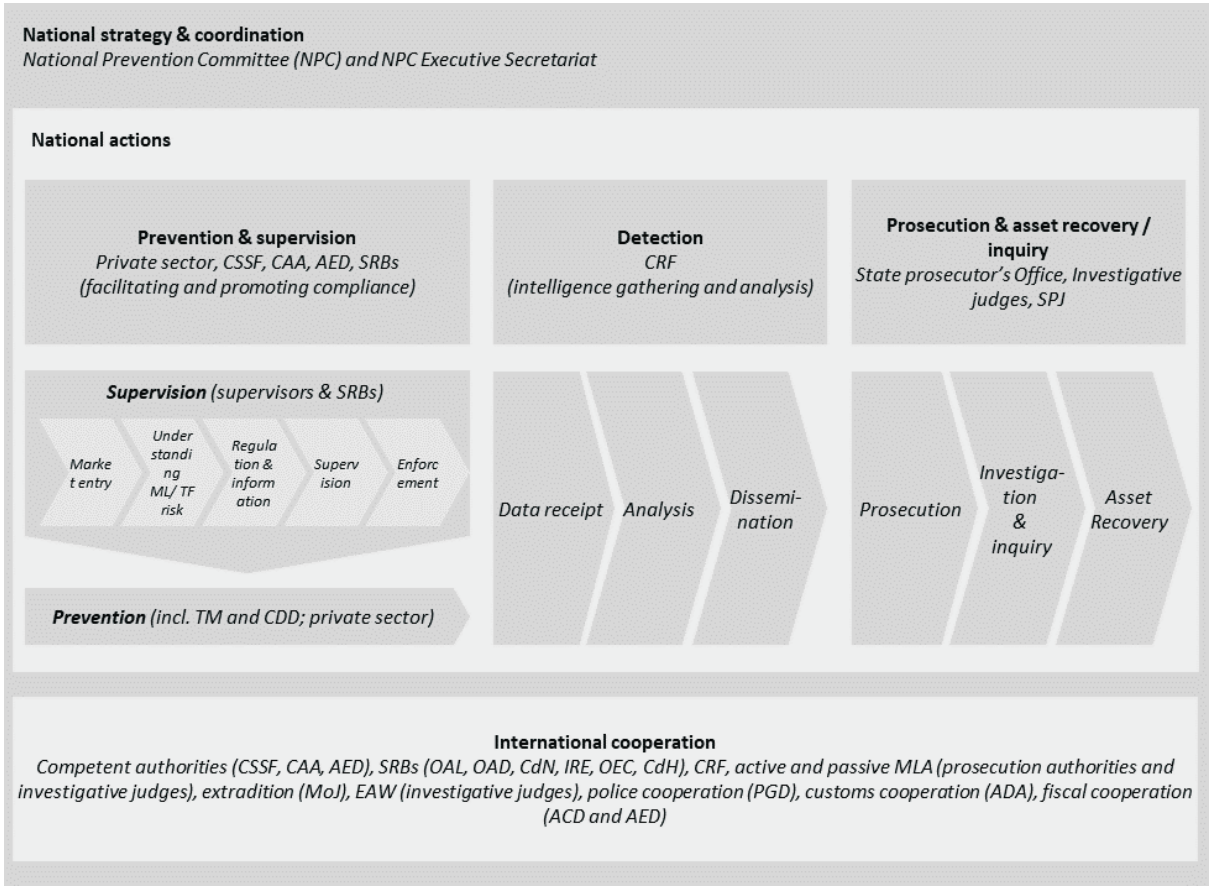
[101] FATF, *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems,* February 2013

Figure 8: Scorecard approach to assess impact of mitigating factors



The framework to structure this part of the exercise was agreed as per Figure 9 (below); this includes five key components, considered to cover all relevant aspects of the AML/CFT institutional set-up in place. National strategy and coordination is required to ensure robustness of national institutional design, coordinate national actions and coordinate cooperation with international bodies and groups. For beginning-to-end control of ML/TF, component parts must cover prevention, detection and prosecution/law enforcement. Prevention/supervision entities facilitate and promote compliance with professional AML/CFT obligations. Detection entities gather intelligence and analyse it to determine if evidence suggests predicate offenses are likely to have occurred. Prosecution/law enforcement entities pursue predicate offenders in the judicial system. Finally, international cooperation provides a solid foundation for national AML/CFT work by promoting best practice exchange, exchange of information, and international coordination.

Figure 9: Mitigating factors framework



Note that compared to the previous NRA, the prevention and supervision sections have been split into separate framework dimensions, with the articulation of the private-sector controls scored under the prevention dimension.

The main institutions, agencies and committees are mapped against each component of the framework to be engaged in the exercise and jointly developed the in-depth assessment to ensure accuracy and completeness. This assessment is then compared against best practice guidelines and peer practices to identify potential gaps and areas for improvement in the current setup.

To assess the impact of mitigating factors, current practices are discussed with concerned entities along a common set of four dimensions: mandate, model, capabilities, and results. This intended to cover the full lifecycle of supervision, detection and enforcement: authorisation to act by relevant governmental bodies (mandate), set-up (model), resource inputs (capabilities) and outputs (results). It is outlined below and in the following figure:

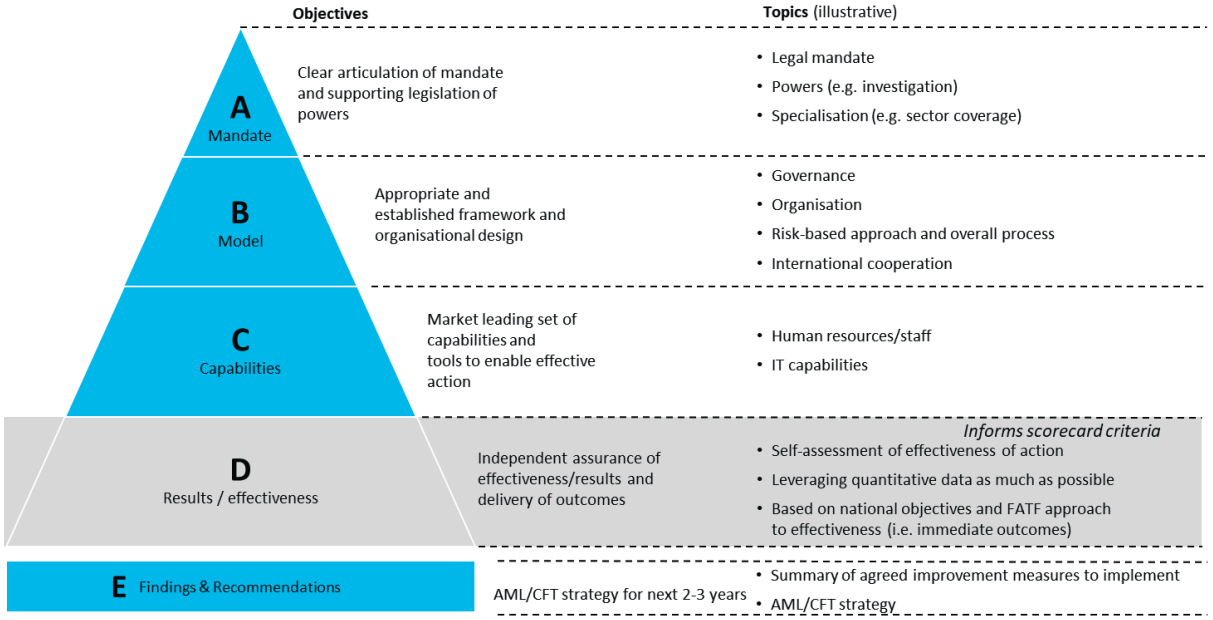
- **Mandate**: When considering a component part's mandate, the legal mandates, powers to source information, powers to sanction, international cooperation, harmonisation of sanctions across similar authorities and whistle-blowing procedures are considered. In addition, comprehensiveness of sectorial coverage by the supervisors and the ability (via data-sharing protocols) to share data with other agencies is also reviewed.
- **Model**: Under the heading of model, the governance framework, organisational design, key functions, operational design, strategic analysis and external cooperation mechanisms are

assessed. The existence and maturity of a risk-based approach to supervision and adequacy of sector-specific regulation are also considered to gauge the appropriateness of the model.

- **Capabilities**: For capabilities, human capital along the dimensions of adequacy of resources and specialist skills are assessed. Furthermore, the database, technology and tools available are also considered.
- **Results**: For results, statistical analyses are chosen based on available data with a view to determine the number and quality of authorisations, sector awareness, inspections (on-site and desk level), sanctions and STRs submissions

Using common dimensions (Figure 10, below) enabled the structuring of the exercise in a coherent way across the many stakeholders involved; it should be noted however some elements of each dimension above are naturally more applicable to some agencies than others.

Figure 10: Dimensions used to assess impact of mitigating factors



The results / effectiveness dimensions are then used to inform the **scorecard criteria**, which include five different criteria:

- Market entry controls
- Understanding of ML/TF risks and AML/CFT obligations
- Prevention/private-sector controls
- Supervision and enforcement
- Detection, prosecution and asset recovery

The different criteria together with data and information inputs examples for them are described in Appendix A.4. Compared to the NRA 2018, the prevention criteria and private-sector controls criteria were retrieved out of the supervision dimensions and added as a separate dimension. The regulation

and information criteria together with understanding of ML/TF risks and AML/CFT obligations were grouped into a single dimension.

3.3.2. Methodology for residual risks

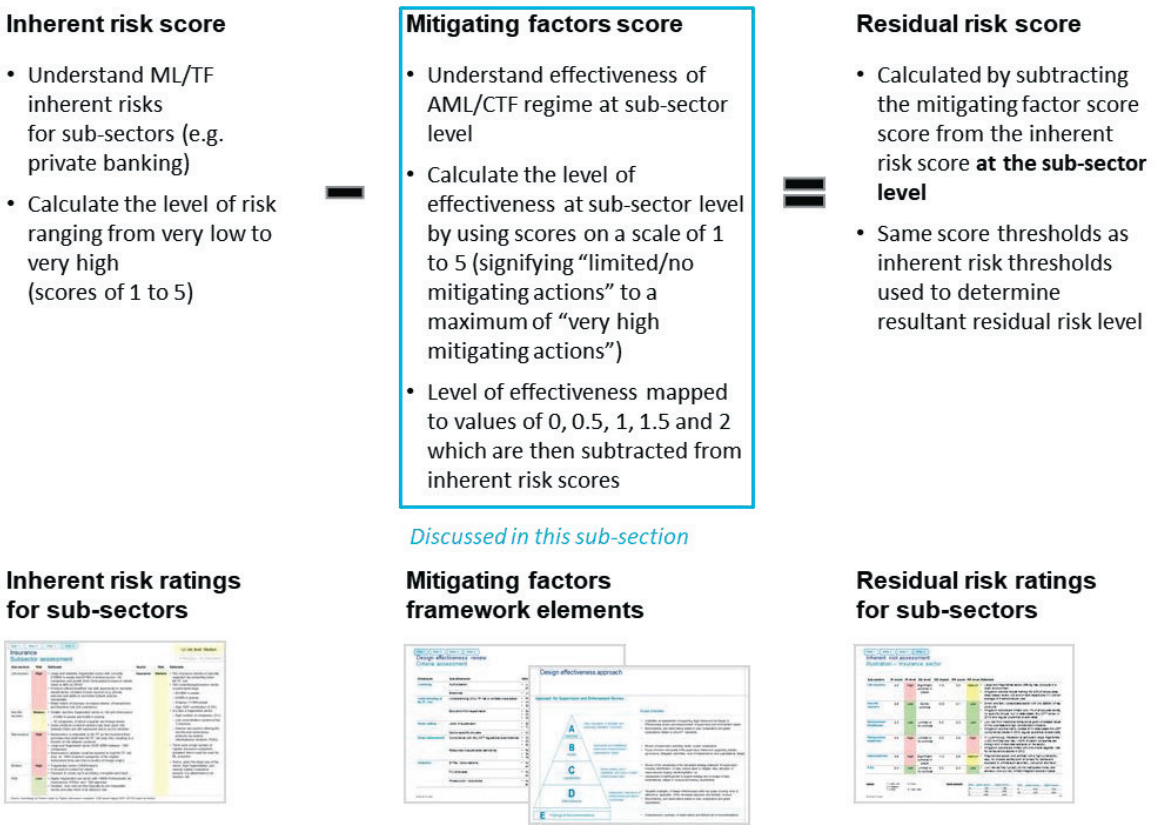
The residual risk assessment considers the level of ML/TF risk after mitigating measures are considered. The residual risk outcomes are used to identify sectors where Luxembourg remains most exposed to ML/TF risks. It thus serves as a basis to develop and prioritise strategic actions that can be undertaken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

The sectorial impact on residual risk depends on the starting level of sectorial inherent risk and the mitigating actions applied to manage these risks. The mitigating actions arise from: the prevention regime (such as supervisors), the detection and prosecution regime (for example CRF, prosecution authorities, investigative judges, judicial police) or the private-sector entities. With regards to the private-sector entities, the supervisory regime sets the rules and regulations but the private sector's level of effectiveness of implementing and complying with these regulations is for instance reflected indirectly in statistics available at the supervisory level (under "Results"). Furthermore, the private sector may also have additional group policies it implements that impact residual risk. It should be noted some mitigating factors affect sectors transversally (e.g. activities by the CRF or the prosecution authorities).

The implications of such a set-up are that deficiencies identified in any of the players impact the sectorial residual risk outcomes. Even if controls and effectiveness of a given regime are best practice, that does not guarantee low levels of sectorial residual risk unless similar standards are observed across the board. This being said, it should be noted if the sectorial inherent risk is very high, even with strong mitigating actions, the residual risk outcome is unlikely to be very low as it is not possible to completely eliminate risks, especially for the most vulnerable sectors.

The calculation of the residual risk per sub-sector (e.g. private banking under the "Banks" sector) is illustrated in Figure 11 (below).

Figure 11: Residual risk calculation



The **inherent risk scores** are determined using the scorecard approach described in the sub-section above on a scale from 1 to 5, ranging from very low risk to very high risk. The scorecard dimensions for sectorial vulnerabilities included size of the sub-sector, fragmentation of the market, ownership/legal structure of the entities, products/activities, client volumes, client risks and interactions channels.

The **mitigating factors impact scores** are calculated using the fact-base obtained under the four dimensions mandate, model, capabilities and results. To enable a more granular assessment of the mitigating factors in place, a scorecard of residual risk criteria is devised, consistent with the four dimensions referred. It includes licensing, understanding of ML/TF risks in the sector, rules setting and rules enforcement by the supervisors and detection and prosecution statistics.

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

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

to a reduction in inherent risk of 0, -0.5, -1, -1.5 and -2, respectively. Note that compared to the previous NRA in 2018, the maximum score was extended from a 4, to a 5. Similarly, the aggregated outcomes were also extended to include an interim level of -1.5 to reflect that some agencies made significant progress.

Finally, the **residual risk score** is assessed by taking the inherent risk score (1 to 5) and subtracting the mitigating factors outcome (i.e. reducing the score by 0, 0.5, 1, 1.5 or 2 points). This results in a residual risk score per sub-sector. The aggregate residual risk level for the sector is then determined by aggregating the residual risk scores across subsectors. An illustration of the residual risk calculation, together with an illustrative example, is provided in Appendix A.4.

3.4. National AML/CFT Strategy

The results of the inherent and residual risk assessment were used to identify improvement opportunities for the current institutional setup to further enhance the AML/CFT measures. These opportunities formed the basis for defining actions for different agencies. Overall, the key outputs of this exercise included detailed action plans with timelines for different agencies, a national action plan and four national strategic priorities, which together form the national AML/CFT strategy. The results of the agency action plans were compiled into a separate document as appendix to the NRA.

Actions were identified, discussed and iterated with each individual agency in bilateral meetings and written correspondence. This included agencies providing an update on the progress against the AML/CFT actions from the previous NRA and sharing their internal ongoing and upcoming initiatives. Those inputs, together with the improvement opportunities identified while assessing the mitigating factors, formed the basis for the creation of actions plans for each agency. Additional consideration was also given to guidance from FATF and other institutions and peer practices. The lists of actions and their timelines were then reviewed and validated by each agency in bilateral meetings. These actions were aggregated and articulated into a comprehensive, national action plan.

Separately, the National AML/CFT Prevention Committee (NPC) identified four areas of particular strategic relevance to focus on. These are the four areas that the NPC has identified as likely to have the greatest impact on further enhancing the effectiveness of the national AML/CFT framework.

The NPC played a key role in articulating the AML/CFT strategy, by formulating and iterating it with agencies for additional feedback and inputs. Going forward, it will support in coordinating the implementation of the strategy in the next years.

4. COVID-19 CRISIS: IMPACT ON THREATS, VULNERABILITIES AND MITIGATING FACTORS

The COVID-19 crisis has led to unprecedented global challenges and economic disruption. Since the emergence of the virus in December 2019 to the time of writing (July 2020) at least half of the world's population has been impacted by some form of lockdown (including, but not limited to: closing of schools; closing of non-essential shops and production; closing of non-essential office spaces; closing of public spaces; curfews; social distancing measures; border closures; and travel restrictions).[102] In Luxembourg, restriction measures were implemented on 12th March 2020.[103]

As many economies face significant downturn, financial flows are likely to diminish (indeed, Luxembourg's national statistics office has stated it will downgrade short-term prospects for the country).[104] However, experience from past crises suggests that in many cases illicit finance continues, and new techniques and channels of laundering money are likely to emerge.[105] An overview of these emerging and evolving ML/TF threats (including predicate offences that generate illicit proceeds which could give rise in particular to ML) and vulnerabilities is provided below.

4.1. ML/TF Threats

Cybercrime and the risks associated with cybersecurity have increased since the outbreak of the pandemic and the imposition of "lockdown" measures driving demand for communication, information and supplies through online channels. Criminals use phishing and ransomware campaigns (such as those included in the case studies below) to exploit the current crisis and capitalise on the anxieties and fears of their victims[106]. CRF's COVID-19 typologies report highlights that working from home creates new risks, as criminals can exploit security loopholes to gain confidential documents, which are then used in sophisticated frauds[107]. Cybercrime threats are likely to continue to be dominant threats as social-distancing measures enhance the reliance on digital services, but the current focus on the distribution of malware and ransomware on targeting particularly affected sectors such as healthcare and education may shift back to attempts to exploit regular businesses as they reopen (either physically or by expanding their business online)[108].

Case Study 1: Phishing scams in Luxembourg using the World Health Organisation (WHO) name[109]

Phishing and email scam campaigns are typically designed to obtain personal information, which can then be used by criminals to steal funds. There has been a significant increase in the amount of scam campaigns related to COVID-19 since January 2020, with research by internet security company Sophos suggesting that the volume of COVID-19 email scams nearly tripled in one week during the end of March, with almost 3% of all global spam now estimated to be Covid-19 related.

[102] See, for instance Euronews (link), Business Insider (link)
[103] See gouvernement.lu for further details (link)
[104] STATEC, *Coronavirus threat becomes a reality,* 2020 (link)
[105] EBA, *Statement on actions to mitigate financial crime risks in the COVID-19 pandemic*, 2020 (link)
[106] EUROPOL, *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic,* 2020 (link)
[107] CRF, *Typologies COVID-19*, 2020 (link)
[108] EUROPOL, *Beyond the Pandemic: how COVID-19 will shape the serious and organised crime landscape in the EU,* 2020 (link)
[109] CSSF, *Circular 20/740*, 2020 (link)

Several of these scams have attempted to use the WHO brand to obtain personal information from victims. In Luxembourg, the government has confirmed one such scam in which senders purporting to be from the WHO or travel agents sent malware-ridden links to a COVID-19 interactive map.

Fraud and forgery has been noted by both domestic and international bodies as a growing threat in the context of the pandemic[110]. The primary fraudulent activities have included: the adaptation of existing telephone or email scams (e.g. criminals calling victims pretending to be hospital officials who claim that a relative has fallen sick and request payments for medical treatment)[111]; supply chain fraud, specifically in relation to personal protective equipment (PPE) and other healthcare products (e.g. an investigation supported by EUROPOL was conducted on the transfer of €6.6 million to a company in Singapore in order to purchase PPE and alcohol gels – the goods were never received);[112] and fraudulent investment scams (e.g. promotions that falsely claim products or services of publicly traded companies can prevent, detect or cure coronavirus)[113].

Other ML/TF threats that have increased or emerged during the COVID-19 crisis include, but are not limited to:

- Corruption and bribery, in particular in relation to government support schemes;
- Insider trading and market manipulation (both as a result of the high volatility of financial markets increasing the risk of persons trying to take advantage of inside information, as well as persons in possession of inside information using insecure communication channels due to remote working arrangements);
- Counterfeiting and piracy, in particular of medicines and other goods, as described in the Case Study 2, below.

Case Study 2: INTERPOL Operation Pangea – Criminals taking advantage of the high demand in hygiene products driven by the COVID-19 outbreak[114]

Operation Pangea, a global operation coordinated by INTERPOL, targeted the trafficking of counterfeit medicines from 3-10 March 2020 as criminals began to take advantage of the high demand in hygiene products driven by the COVID-19 outbreak. The operation involved 90 countries worldwide and resulted in 121 arrests.

During the operation, authorities around the world seized 37 000 unauthorised and counterfeit medical devices (mostly surgical masks and self-testing kits for HIV and glucose monitoring) and €13 million in potentially dangerous pharmaceuticals (such as unauthorised antiviral medications and the antimalarial medicine chloroquine). Painkillers and antibiotics also represented a significant portion of the seizures.

[110] See, for instance, CSSF, *Circular 20/740*, 2020 (link); EUROPOL, *Pandemic profiteering – How criminals exploit the COVID-19 crisis*, 2020 (link); and FATF, *COVID-19-related Money Laundering and Terrorist Financing* (link)

[111] INTERPOL, *INTERPOL Warns of Financial Fraud Linked to COVID-19,* 2020 (link)

[112] EUROPOL, *How criminals profit from the COVID-19 pandemic*, 2020 (link)

[113] EUROPOL, *COVID-19: Fraud*, 2020 (link)

[114]INTERPOL, *Rise of fake "corona cures" revealed in global counterfeit operation*, 2020 (link)

4.2. ML/TF Vulnerabilities

Whilst it is possible that specific areas across Luxembourg's financial and non-financial sectors could be exploited by the emerging ML/TF threats described above, there are specific vulnerabilities that are particularly relevant in the context of COVID-19.

Online financial services and virtual assets: The increase in online purchases as a result of the social-distancing measures is likely to lead to the increase in both the volume and value of online payments services, including the use of internet banking. This may create more opportunity for criminals to conceal illicit funds within a greater amount of legitimate payments made online. FATF has highlighted the continuing ML/TF risks associated with virtual assets to move and conceal illicit funds[115].

Entities in financial distress: The contraction in Luxembourg's economic activity as a result of the global pandemic could place some entities in distress (e.g. corporates and SMEs), which in turn creates opportunities for them to be exploited by criminals seeking to launder illicit proceeds (e.g. if a corporate is required to make a significant payment by a credit institution, the corporate may be forced to accept proceeds from an organised criminal group in exchange for an ownership share of the business, enabling the integration of illicit proceeds). Furthermore, credit institutions may revalue existing collateral or request additional collateral to be placed against existing or new loans – if controls on the origin or source of funds and wealth are relaxed to obtain this, it could facilitate the entry of illicit proceeds into the financial system[116].

Delivery of government or international financial assistance, particularly through non-profit organisations: Luxembourg has provided support to businesses to counter the economic impact of COVID-19[117]. International financial institutions report that there is a risk that criminals or terrorists may fraudulently claim or misdirect such funds. Corruption in procurement or aid delivery channels could also impact international financial assistance[118], particularly relevant for non-profit organisations (NPOs). FATF has highlighted that most NPOs carry little or no ML/TF risk, though CSSF notes that where there are increased financial flows through NPOs to higher risk countries, there may be an increased risk of illicit activity (including TF), and that there remains the potential for tax advantages afforded by charitable donations to be misused by those seeking to engage in ML activities[119].

[115] FATF, *COVID-19-related Money Laundering and Terrorist Financing* (link)
[116] CSSF, *Circular 20/740*, 2020 (link)
[117] For further details see: European Commission, *Temporary Framework for State aid measures to support the economy in the current COVID-19 outbreak, 2020* (link)
[118] FATF, *COVID-19-related Money Laundering and Terrorist Financing* (link)
[119] CSSF, *Circular 20/740*, 2020 (link)

4.3. Mitigating factors

FATF has set out a range of mitigating factors and AML/CFT responses to the evolving risks impacted by COVID-19[120]. Those most important for Luxembourg include (but are not limited to): coordinate domestically and continue to cooperate internationally to assess the ongoing impact of COVID-19 on AML/CFT risks; strengthen communication and monitoring of the private sector by engaging on the application of their AML/CFT measures; and continue to encourage a risk-based approach to CDD to address practical issues. For example, in order to inform private sector entities, the CSSF published a circular on the implications of COVID-19 on AML/CFT issues (10 April 2020) and held a specific workshop beginning of May 2020 in order to further raise awareness in the specific sector of collective investments. The outcome of the workshop was published in the form of a presentation on the website of the CSSF and had been shared with IOSCO members in the context of CSSF's on-going cooperation with its international partners[121]. CRF also published COVID-19 typologies (2 April 2020). Private-sector entities should continue to strengthen their understanding of the developing risks by engaging directly with authorities and reading these and other relevant publications[122]. It is noted that as the COVID-19 pandemic continues to evolve, additional ML/TF threats and vulnerabilities may emerge – the mitigating factors described above serve also to prepare the country for these dynamic risks.

[120] FATF, *COVID-19-related Money Laundering and Terrorist Financing* (link)

[121] CSSF, Presentation: AML/CFT supervision in the Collective Investment Sector during the COVID-19 situation (link)

[122] At the time of writing (June 2020), COVID-related guidance has been published and/or distributed by a number of relevant bodies, including but not limited to: FATF; EBA; EUROPOL; INTERPOL; CAA; IRE; OEC and AED

5. INHERENT RISK – THREATS ASSESSMENT

5.1. Summary

As described in the methodology section, threats are assessed on a scale of 1 to 5 (very low, low, medium, high, and very high), and analysed across:

- Money laundering (ML; domestic and foreign crimes)[123]
- Terrorism and terrorist financing[124] (TF; also predicate offences to money laundering)

It should be noted threats are analysed within the inherent risk assessment component of the NRA; that is, in the absence of mitigating factors and controls for ML/TF (see also methodology section of NRA for more detail).

Money laundering (domestic and foreign crimes)

Money laundering is the highest threat for Luxembourg, in particular money laundering of foreign criminal proceeds, due to Luxembourg's position as a major non-domestic European financial centre (note: it is commonly observed that criminal proceeds are laundered in different locations from where crimes are perpetrated[125]; some estimates consider that as much as 30% of all criminal proceeds globally are laundered abroad[126]).

The threat of money laundering of proceeds of domestic crimes is estimated to be significantly smaller, due to Luxembourg's relatively low crime rate and limited presence of organised crime. However, the Grand-Duchy's wealth, its economy (including payments, investments, cyber and logistics providers), its high number of international institutions and its central location in Europe increase the ML threat level for certain types of crime. While some crimes might be perpetrated domestically, this does not necessarily imply that their proceeds are laundered domestically. They might instead be taken abroad (e.g. offences committed by foreign organised crime groups, taking proceeds outside Luxembourg). Given the common market, criminals can easily cross the border to France, Germany or Belgium by car or public transport.

Terrorism and terrorist financing (TF)

The threats of terrorism and terrorist financing are assessed as medium overall; despite the likelihood of an attack being low in Luxembourg, the consequences could be very high.

[123] ML is criminalised through three specific legal provisions, as defined in Article 506-1 of the Penal Code (and Article 8-1 of the 1973 Drug Trafficking Law). The offence of money laundering is in essence the act of knowingly facilitating deceit as to the nature, origin, location, disposal, movement or ownership of any kind of asset obtained criminally. Note that ML always needs to be based on a predicate offence that served to generate the illegal proceeds. In a certain way, ML is part of the predicate offence itself as soon as the perpetrator is detaining the proceeds obtained from the offence. For further details, see Prosecution section.

[124] As defined in the Penal Code, Article 135. Terrorist financing specifically is captured in Article 135-5. For further details, see Prosecution section.

[125] See for instance, FATF, *FAQ on money laundering*, (link)

[126] See for instance, R. W. Baker, *Capitalism's Achilles Heel: Dirty Money and How to Renew the Free-Market System*, 2005 (link)

Terrorism: Despite no previous terrorism attacks and no known terrorist groups in Luxembourg, Luxembourg raised its level of terrorism threat to 2 (on a scale of 4) in 2015, in light of recent terrorism events in neighbouring countries[127]. The raised threat level was kept since then.

Terrorist financing: Terrorist financing is a more likely threat to Luxembourg than terrorism, given the country's open economy. Still, both threats are closely connected and deemed overall moderate relative to ML. Accordingly, there are few TFTR and TFAR[128] reported to the CRF (across all submitting entities), Luxembourg's FIU. The risk of a sector (e.g. payments, non-profit organisations) or Luxembourg's financial centre being targeted by foreign terrorist groups for their financing purpose is however not to be excluded.

Table 8 below gives an overview of threats across money laundering and terrorism and terrorist financing, with further details in the sections below.

Table 8: Inherent risk – Summary of threats

	External exposure (75 % weight)	Domestic exposure (25 % weight)	Weighted average exposure
Money laundering (*average ML threat across external and domestic exposure*)	**Very high**	**Medium**	**Very high**
Terrorism and terrorist financing (*also as predicate offences to ML*)	**Medium**	**Medium**	**Medium**

COVID-19 impact on threats

The COVID-19 crisis has led to unprecedented global challenges and economic disruption. Since the emergence of the virus in December 2019 to the time of writing (July 2020), at least half of the world's population has been impacted by some form of lockdown.[129] In Luxembourg, restrictions were implemented on 12 March 2020.[130] As many economies face significant downturn, financial flows are likely to diminish (indeed, Luxembourg's national statistics office has stated it will downgrade short-term prospects for the country)[131]. However, experience from past crises suggests that in many cases illicit finance will continue, and new techniques and channels of laundering money are likely to emerge.[132] In particular, cybercrime and the risks associated with cyber security have increased since the outbreak of the pandemic and the imposition of lockdown measures driving demand for communication, information and supplies through online channels. Fraud and forgery have also been noted by both domestic and international bodies as a growing threat in the context of the pandemic[133]. The primary fraudulent activities have included: the adaptation of existing telephone or email scams;

[127] The level of terrorism threat was raised after the Paris attacks in November 2015, and kept at this level after the Brussels attacks in March 2016 as per communication by the Ministry of State. Level 2 (medium threat) defines a real yet abstract terrorist threat; it consists of increasing vigilance against an imprecise threat and to implement measures of vigilance, prevention and protection of variable and temporary intensity. See *Ministère d'Etat Luxembourg*, Press Announcement on 23/03/2016 (link).

[128] Terrorism Financing Transaction Report (TFTR) and Terrorism Financing Activity Report (TFAR).

[129] See, for instance Euronews (link), Business Insider (link)

[130] See gouvernement.lu for further details (link)

[131] STATEC, *Coronavirus threat becomes a reality,* 2020 (link)

[132] EBA, *Statement on actions to mitigate financial crime risks in the COVID-19 pandemic*, 2020 (link)

[133] See, for instance, CRF, *Typologies COVID-19*, 2020 (link); CSSF, *Circular 20/740*, 2020 (link); EUROPOL, *Pandemic profiteering – How criminals exploit the COVID-19 crisis*, 2020 (link); and FATF, *COVID-19-related Money Laundering and Terrorist Financing* (link)

supply chain fraud, specifically in relation to personal protective equipment (PPE) and other healthcare products; and fraudulent investment scams[134]. Some detail on key threats likely impacted by the pandemic are highlighted throughout the section; however, a more detailed assessment is provided in the section 4 of the NRA on the impact of the COVID-19 crisis on threats, vulnerabilities and risks.

5.2. Money laundering

National exposure to ML threats map

An overview of the ML threat level per category – including a breakdown per predicate offence – is provided in table 9 below. Threats have been assessed along a list of predicate offences in line with FATF crime categories[135]; these map to granular predicate offences (*"infractions primaires"*) under Luxembourg law. A full mapping table can be found in the "Prosecution" section later below in the NRA document.

The overall threat assessment is based on a weighted average between domestic and foreign exposure, with 25% and 75% weights respectively. Given Luxembourg's open economy and large financial sector, the country is more exposed to ML from criminals abroad than domestically. For simplicity, the weighting is assumed to be constant across predicate offences. The rest of this section provides a more detailed assessment ("bottom up") per predicate offence, split into domestic and foreign exposure to ML.

Table 9: National exposure to ML threats map[136]

Designated predicate offense	External exposure (75%)	Domestic exposure (25%)	Weighted average exposure
Money laundering (average ML threat)	**Very high**	**Medium**	**Very high**
Fraud and forgery	**Very high**	**High**	**Very high**
Tax crimes	**Very high**	**Medium**	**Very high**
Corruption and bribery	**Very high**	**Medium**	**Very high**
Drug trafficking	**High**	**Medium**	**High**
Participation in an organised criminal group & racketeering	**High**	**Medium**	**High**
Sexual exploitation, including sexual exploitation of children	**High**	**Medium**	**High**
Cybercrime	**High**	**Medium**	**High**
Counterfeiting and piracy of products	**High**	**Low**	**High**
Smuggling	**High**	**Low**	**High**
Robbery or theft	**Medium**	**High**	**Medium**
Trafficking in human beings and migrant smuggling	**Medium**	**Medium**	**Medium**
Illicit arms trafficking	**Medium**	**Low**	**Medium**
Insider trading and market manipulation	**Medium**	**Low**	**Medium**

[134] EUROPOL, *COVID-19: Fraud*, 2020 (link)

[135] FATF NRA Guidance, February 2013, Annex I (link).

[136] This assessment is based on a mix of research and data available, expert judgement, bilateral meetings and a workshop group discussion with judicial authorities. Exposure to predicate offences constituting the threats was broadly assessed along a set of criteria, namely the probability of the crime occurring, proceeds of the crime if occurring (including size and form of proceeds, and complexity/expertise of ML and geography, where available), and the human, social and reputational impact (the latter for domestic exposure only).

Designated predicate offense	External exposure (75%)	Domestic exposure (25%)	Weighted average exposure
Illicit trafficking in stolen and other goods	Medium	Low	Medium
Extortion	Low	Medium	Low
Environmental crimes	Low	Low	Low
Murder, grievous bodily injury	Low	Very Low	Low
Kidnapping, illegal restraint, and hostage taking	Low	Very Low	Low
Counterfeiting currency	Low	Very Low	Low
Piracy	Low	Very Low	Low
Terrorism and terrorist financing	**Medium**	**Medium**	**Medium**

5.2.1. External exposure: Money laundering of proceeds of foreign crimes

Money laundering of proceeds of foreign crimes is the most significant ML threat for Luxembourg, given its position as a global financial centre and the low level of local criminality. The magnitude, diversity and openness of financial flows transiting through and parked in Luxembourg contribute to this exposure. This is supported by data from the judicial authorities, international studies and expert assessment from the country's authorities.

The likelihood of Luxembourg being misused or abused for ML of proceeds of foreign crimes is very high, given the Grand-Duchy's role as one of the world's main financial hubs. In fact, Luxembourg is ranked 25th on the Global Financial Centres Index[137] and has a high number of financial flows in and out of the country, with and from different geographies. OECD reports that Luxembourg has a very high incoming FDI stock as a percentage of GDP in 2019 with 313% compared to an EU average of 67%[138]. STATEC data from 2018 suggests that about 31% of foreign FDI come from offshore financial centres[139], which presents a potentially higher threat for ML. Luxembourg also has a very large banking sector as a percentage of GDP (about 1300% with over €901 billion banking assets as of March 2020), with 128 different credit institutions from 27 different countries[140]. According to Tax Justice Network's 2018 ranking, Luxembourg has the sixth highest Financial Secrecy Index out of 112 countries, sitting between Singapore and Japan[141] . This is based on a moderate secrecy score and the very large size of the financial sector: Luxembourg is rated to have a very large share (12%) of global offshore financial services[142]. It should be noted however that Luxembourg's large share of financial flows relative to its size, as depicted in these several studies, should also be put into context with its central role for these services in the EU common market.

[137] The Global Financial Centres Index 26, September 2019

[138] OECD Benchmark definition, 4th edition (BMD4): Foreign direct investment: positions, main aggregates (Outward/Inward, % of GDP, 2019 or latest available) (link)

[139] STATEC, Net annual income of on FDI of Luxembourg (according to the extended directional principle; in millions of euros; 4th OECD benchmark definition) (source)

[140] Banque Centrale du Luxembourg, *Statistiques : Etablissements de crédit ; „tableau 11.01" and „tableau 11.05"* as of March 2020 (link)

[141] Tax Justice Network, Financial Secrecy Index 2020, Results (link)

[142] Tax Justice Network, *Financial Secrecy Index 2020, Narrative Report on Luxembourg*, 2020 (link)

The magnitude of the financial sector and its share of foreign financial flows contribute to the proceeds of foreign crimes to be potentially laundered in Luxembourg. Moreover, the sophistication employed by money launderers is estimated to be very significant as well. International studies and guidance point towards criminal proceeds being often laundered in distant places from where crimes were perpetrated to try to conceal the origin of funds[143]. Estimates are varied, but for example, one study[144] estimates that as much as 30% of worldwide unlawful earnings are laundered cross-border, making countries with significant shares of foreign direct flows more vulnerable.

ML of foreign crimes accounts for a significant share of Mutual Legal Assistance (MLA) and asset seizures by Luxembourg authorities. Across all crimes, the prosecution authorities report having received a total of 1 701 MLAs on aggregate in the past three years of 2017–2019, of which 362 are related to self-laundered (SL) ML[145]. Note, it is estimated that most ML MLA requests are SL-related, however there are also MLA requests that arise from third-party or stand-alone ML. Data from the prosecution authorities show seizures following MLAs across all crimes in the past three years (2017–2019) of ~€311.5 million, compared to ~€92.1 million for domestic cases[146].

As in any other country, if significant amounts are to be laundered via Luxembourg this could indirectly encourage criminal activities elsewhere with significant human, social and reputational impacts. Citizens and companies abroad are negatively impacted if criminals can launder the proceeds of their crimes in other countries. Africa alone is estimated to lose more than $50 billion annually through illicit financial outflows[147]. The reputational and social costs for Luxembourg would be significant, in particular if the country is portrayed negatively for being used for ML, given its economic model centred on the financial sector; this is Luxembourg's largest economic sector with ~50 900 employees[148] and 23% of GDP[149].

Split of threat by predicate offence

The sub-sections below provide an overview of the overall threat level of ML of proceeds of foreign crimes, by foreign predicate offence. It is worth noting that the split of threats is delineated on a best-effort basis, as it is inherently difficult to ascertain the origin, geography and detail of the predicate offences associated with possible illicit proceeds flowing through the country.

The most likely external threats for Luxembourg in terms of ML are believed to be: fraud and forgery; tax crimes; corruption and bribery; and drug trafficking. In fact, these four crimes represent more than 70% of estimated criminal proceeds generated globally[150], ~45% of seizures following MLA to the prosecution authorities in 2017–2019[151], and 57% of MLA received by the prosecution authorities in 2017–2019[152]. This is also in line with expert assessment from the country's judicial authorities.

[143] See for example: UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011 (link), or FATF, *FAQ on money laundering* (link)

[144] R. W. Baker, *Capitalism's Achilles Heel: Dirty Money and How to Renew the Free-Market System*, 2005 (link)

[145] Parquet Général Statistical Service, Data received in March 2020

[146] Parquet Général Statistical Service, Data received in March 2020

[147] UNECA, *Illicit Financial Flows from Africa*, 2015 (link)

[148] STATEC, Emploi salarié intérieur par branche d'activité - données désaisonnalisées 1995 – 2019 (4e trimestre 2019) (link)

[149] STATEC, Valeur ajoutée brute aux prix de base par branche (NaceR2) (prix courants) (en millions EUR) 1995 – 2019 (link)

[150] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011 (link)

[151] Parquet Général Statistical Service, data received in March/April 2020

[152] Parquet Général Statistical Service, data received in July 2020; note that besides requests for LAR received by the prosecution authorities, other Luxembourg authorities (e.g. CRF, Asset Recovery Office, Police) also receive other "foreign requests" for cooperation and/or information sharing.

5.2.1.1. Fraud and forgery

Fraud and forgery are estimated to generate ~12% of crime proceeds globally; in some of Luxembourg's neighbouring countries, this figure is significantly higher (e.g. in Germany and the Netherlands)[153].

Luxembourg's position as a payments, investment and cyber hub increases the likelihood that criminals (in Luxembourg and abroad) commit fraud involving Luxembourg-based institutions (wittingly or unwittingly), and potentially launder the proceeds of that fraud via Luxembourg:

- **Payments hub**: The ECB reports that 74% of EU e-money transactions have been made in Luxembourg in 2018[154], reflecting the fact that PayPal and Amazon Payments Europe have established their European headquarters in the country. The very high number of electronic STR and SAR (33 399 in 2019) reported by the CRF for fraud and forgery supports this[155].
- **Investment hub**: According to CSSF data[156], of 97 investment firms established in Luxembourg, 82 have the license of private portfolio manager, with 68 of them exercising relevant activities. They have €40.6 billion assets under management (AuM), numerous clients, substantial international business (~95% of clients are international) and foreign ownership (~37% of firms are owned or controlled by foreign non-EU persons/entities)
- **Cyber hub**: Technology leaders such as Amazon, Skype and PayPal all have their European headquarters in Luxembourg[157]. Moreover 23 data centres (~50 000 sq. m.)[158] are established in the Grand-Duchy. Cyber fraud, often coupled with cyber-crime, is believed to be increasing; for instance, Thomson Reuters estimates cyber-crime to generate €1 trillion per year globally[159].

This assessment is in line with the very high figures reported by the prosecution authorities for fraud: they received 796 MLA in 2017-2019 (of which 204 self-laundered ML-related) and have seized assets worth €176.4 million following MLA on fraud and forgery in that period. In 2019, the prosecution authorities seized ~€88.6 million for international fraud and forgery cases[160].

As illustrated in Case study 3, fraudulent crimes often involve another type of infraction, in this example cybercrime.

[153] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011 (link)
[154] ECB, Payment Statistics (full report); Table 7.1 Number of payments per type of payment service, 2018 figures (link)
[155] CRF annual report 2019
[156] CSSF data provided for Sectorial vulnerabilities of the NRA in 2019-20
[157] Luxembourg for Finance, *Why Luxembourg?* Website (link)
[158] Datacentres in Europe, Website (link)
[159] Thomson Reuters, *Cybercrime, Financial fraud and money laundering: understanding the new threat landscape*, 2013 (link)
[160] Data received from Parquet Général Statistical Service in March/April 2020

Case Study 3: Fraudulent transactions by way of fake email addresses[161]

A Luxembourg company uses an accountant for its payments. For a payment to be executed, an employee of the company must send the payment order to the accountant to be countersigned, who then sends it to the bank for execution. In the present case, the fraudsters initially hacked into the victim's e-mail account and, probably by analysing the exchanges contained therein, (i) determined the payment procedure in force and (ii) took possession of previous payment examples that one of the company's employees had left in his mailbox in PDF format.

The fraudsters then prepared two false payment instructions, of ~€250 000 and €200 000, by using the victim's style, shape and logo and by affixing a false signature of the company's CEO. These payment orders were finally sent via the hacked e-mail address to the accounting company, which forwarded them to the bank that executed them. It should be noted that in the e-mail addressed to the accountant, written in a familiar tone that was probably customary, the emphasis was placed on urgency, but without exaggerating. It said "It's quite urgent..."

In this case, the fraudsters had, in addition to hacking into the employee's e-mail address, also created a domain name very similar to that of the victim, probably to support their actions. They changed the “u” to a “v”, creating the domain name: levisvel.com resembling the original levisuel.com. They then used e-mails that closely resembled the originals: pierre.dupont@levisvel.com instead of pierre.dupont@levisuel.com81

Importantly, fraud and forgery have been noted by both domestic and international bodies as growing threats in the context of the COVID-19 pandemic[162]. The primary fraudulent activities have included: the adaptation of existing telephone or email scams (for example criminals calling victims pretending to be hospital officials, who claim that a relative has fallen sick and requests payments for medical treatment)[163]; supply-chain fraud, specifically in relation to personal protective equipment (PPE) and other healthcare products (for example an investigation supported by EUROPOL was conducted on the transfer of €6.6 million by a company to a company in Singapore in order to purchase PPE and alcohol gels – the goods were never received)[164]; and fraudulent investment scams (promotions that falsely claim products or services of publicly traded companies can prevent, detect or cure coronavirus)[165].

5.2.1.2. Tax crimes

Tax crimes are estimated to generate about 30% of crime proceeds globally according to UNODC. In some of Luxembourg’s neighbouring countries, this is estimated to be even higher. In Germany, for example, the largest source of unlawful income is tax and excise evasion (44% of the total unlawful proceeds of $80 billion in 2007/2008)[166]. While the level of tax and banking transparency has been increased significantly in recent years[167], there is a risk that foreigners continue trying to abuse or

[161] CRF Annual Report, 2017

[162] See, for instance, CSSF, *Circular 20/740*, 2020 (link); EUROPOL, *Pandemic profiteering – How criminals exploit the COVID-19 crisis*, 2020 (link); and FATF, *COVID-19-related Money Laundering and Terrorist Financing* (link)

[163] INTERPOL, *INTERPOL Warns of Financial Fraud Linked to COVID-19,* 2020 (link)

[164] EUROPOL, *How criminals profit from the COVID-19 pandemic*, 2020 (link)

[165] EUROPOL, *COVID-19: Fraud*, 2020 (link)

[166] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011 (link)

[167] For example, by the Law of 23 December 2016 implementing the 2017 tax reform, as well as tax transparency initiatives promoted by the Direct tax administration in Luxembourg; see also ACD section (under Detection) for details on these.

misuse Luxembourg financial institutions and DNFBPs (i.e. lawyers, accountants) to avoid paying taxes in their home country. The prosecution authorities received 156 MLA on tax crimes in 2017-2019, of which 72 were self-laundered ML-related, and have seized assets worth €7 million following MLA in that period)[168].

The following case studies (below) illustrate two different examples of tax crimes, first through the provision of third-party accounts, and then by way of a loan.

Case Study 4: Provision of third-party accounts, private banking and tax fraud[169]

A Belgian national, residing for tax purposes in Thailand, holds an account with a Luxembourg bank, from which he regularly transfers funds to his daughter's bank account. These funds would come from a donation as well as the sale of land and buildings for a total amount of € 2.1 million.

Between 2015 and 2017, the account is debited of a total of €1 million to a law firm specialising in civil and property law in Spain for the acquisition of three apartments. In 2016, the person concerned stays in Belgium for six months. Then he returns to Thailand and regularly travels to Spain, the United States and Belgium.

As a result of all these elements, the bank is unable to establish his tax compliance and terminates the business relationship.

Case Study 5: Doubts on economic reasons for a loan[170]

A company whose tax residence is in Lichtenstein has a bank account with a Luxembourg bank. This company is requesting a loan of $10 million to be transferred to the private account of the economic beneficiary, resident for tax purposes in Ecuador, guaranteed by the latter's private funds which would be the result of his professional activity. According to open sources, the economic beneficiary is reportedly the president of an Ecuadorian company linked to corruption cases in Ecuador, and his wife would be politically exposed. However, in Liechtenstein, the granting of a loan by a company to its beneficiary would be considered as a distribution of hidden profits.

5.2.1.3. Corruption and bribery

Corruption and bribery are estimated to generate ~2% of crime proceeds globally according to UNODC. While this is less significant than the threats discussed above, Luxembourg appears to have been particularly impacted by this threat over recent years.

In the years 2018 and 2019, the CRF blocked significant amounts relating to corruption and bribery: about €64.1 million in 2018 and €10.5 million in 2019. Most of these freeze orders were decided in international cases, in order to give the foreign authorities concerned the possibility to send an MLA request for the judicial seizure of the funds. In total, the prosecution authorities received 63 MLA on corruption and bribery in 2017–2019, of which 39 are self-laundered ML-related, and seized assets of

[168] Parquet Général Statistical Service, data received in March/April 2020
[169] CRF Annual Report, 2017
[170] CRF Annual Report, 2017

€130 million following MLA[171]. In 2019, the prosecution authorities seized ~€97.4 million following convictions in international corruption and bribery cases[172].

The two case studies (below) illustrate examples of corruption and bribery involving external clients or transactions.

Case Study 6: Corruption and misappropriation of public funds[173]

A Luxembourg company, with no real activity, received funds from a bank account held by an offshore company with a European bank into its bank account held with a Luxembourg bank. The transfer of funds was justified by a shareholder loan agreement. The funds were subsequently used to invest in the real estate sector in Luxembourg. The beneficial owner of both companies was a person who was officially active in the construction and civil engineering sector abroad. The FIU's analysis identified close links with another person listed in a KYC database and who was also linked to a suspicion of money laundering in the same country. International cooperation has been initiated to identify the economic origin of the funds that were used to invest in the real estate sector in Luxembourg.

Case Study 7: Suspicious transactions and corruption[174]

A local bank detected, on the basis of alert analyses generated by a monitoring tool, a series of suspicious transactions linked to companies registered in particular in Costa Rica, whose sole economic beneficiary was a person of Uruguayan nationality.

First, it was found that the transactional behaviour of the concerned companies, which, when the accounts were opened, were presented as operating companies (consulting, financial advice, trading), did not correspond to the use of the accounts as described by the client when entering into the relationship. On the contrary, the analysis of the activity of the accounts revealed numerous IN/OUT transfers, documented by contracts often with very vague content (consulting) and not always consistent with the activities expected of the companies.

Secondly, the FIU carried out an analysis of the history of the relevant accounts, which revealed that at least one of the accounts had been used to receive funds from a Swiss account whose holder was allegedly involved, according to public sources, in a corruption scandal in Latin America for having obtained bribes amounting to $785 000 in his capacity as director of the body responsible for infrastructure and public transport in that country in return for favours from his office.

An exchange with relevant counterparts confirmed the suspicion and identified the origin of the funds. The judicial authorities of the country in question subsequently forwarded an international rogatory letter to the Luxembourg judicial authorities, which resulted in the seizure of funds in Luxembourg, which had previously been frozen by the FIU.

[171] Parquet Général Statistical Service, data received in March/April 2020
[172] Parquet Général Statistical Service, data received in March/April 2020
[173] CRF Annual Report, 2018
[174] CRF Annual Report, 2018

The case study below, from the CSSF thematic work in its Private Banking Sub-sector Risk Assessment (SSRA), illustrates an example of private banks' exposure relating to foreign corruption and bribery.

Case Study 8: Suspicious transactions involving the Estonian branch of Danske Bank A/S

Context

Following the publication of media reports about significant volumes of suspicious transactions involving the Estonian Branch of Danske Bank A/S (Danske Estonia), CSSF contacted a number of banks to obtain more information on (1) potential transactions with Danske Estonia; (2) banks' conclusions from their own investigation of their monitoring of these clients and transactions; and (3) any actions taken or proposed to be taken as a result of their investigation. The main purpose of CSSF's intervention was to ascertain whether banks had respected their professional obligations and monitored their clients and transactions adequately. Banks were also requested to review the effectiveness of their processes and procedures to ensure they were adequate to detect similar risks going forward.

CSSF's work showed that (consistently with the NRA), Luxembourg's banking sector is exposed to ML/FT risks from its international clientele and the high volume and frequency of cross-border flows.

Findings and conclusions

The findings from CSSF's investigation underline that as an international financial centre with a high degree of political stability, Luxembourg may be attractive for wealthier clients, including those whose wealth may originate from higher-risk jurisdictions. These wealthy, higher-risk clients often set up multiple accounts with multiple banks and are introduced to these banks through intermediaries. They often seek out private banking departments of banks, even when their banking activity can be very transactional, complex and difficult to assess.

Private banks must operate under a clearly defined ML/FT risk appetite and ensure their risk-based approach considers all relevant risk factors and weights them appropriately (in particular those inherent to clients and geographical origin of assets). Undervaluing client risk may lead to insufficient due diligence and monitoring measures being applied, exposing the bank to financial sanctions and reputation risk.

Corruption and bribery have been noted as growing threats in the context of the COVID-19 pandemic, particularly in relation to government support schemes. Further detail is provided in section 4 of the NRA on the impacts of COVID-19.

5.2.1.4. Drug trafficking

Drug trafficking is estimated to generate ~30% of crime proceeds globally according to UNODC[175], and is believed to be the most important foreign crime in terms of ML together with tax crimes.

Luxembourg may be exposed to this threat externally both via financial flows from abroad, and due to its proximity with countries estimated to have sizable drug trafficking activity, such as Germany,

[175] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011 (link)

France, and the Netherlands given their market sizes[176]. The prosecution authorities received 102 MLA on drug trafficking in 2017–2019, of which 27 are related to self-laundered ML, and seized assets of ~€106 000 following MLA for drug trafficking over that period[177].

5.2.1.5. Other foreign crimes

There are a number of other foreign crimes that are deemed high threat for ML of proceeds in Luxembourg, including participation in organised criminal groups and racketeering; counterfeiting and piracy of products; sexual exploitation, including sexual exploitation of children; and smuggling. All remaining predicate offences have been classified as being less significant in terms of the threat of ML of proceeds of foreign crimes.

The table (below) provides an overview of the external threat assessment across all foreign crimes, detailing the likelihood, size and overall threat level across all threats.

[176] See for instance, Organized Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

[177] Parquet Général Statistical Service, Data received in April 2020

Table 10: Overview of threat assessment of all foreign crimes

Predicate offence	Data/evidence summary	Likelihood/ probability	Size/ proceeds	Overall threat level
Fraud and forgery	• Estimated to generate ~10% of crime proceeds globally, and in some of Luxembourg's neighbouring countries this figure is significantly higher • Prosecution authorities received more than1 000 MLA for fraud and forgery in 2015–2019, 318 of which are SL ML-related • Luxembourg's position as a payments, investment and cyber hub increases the likelihood that criminals (in Luxembourg and abroad) commit fraud involving Luxembourg-based institutions (wittingly or unwittingly), and potentially launder the proceeds of that fraud via Luxembourg	**Very high**	**Very high**	**Very high**
Tax crimes	• Estimated to generate about 30% of crime proceeds globally; in some of Luxembourg's neighbouring countries, this is estimated to be even higher. In Germany for example, the largest source of unlawful income is tax and excise evasion (44% of the total unlawful proceeds of $80 billion in 2007/2008) (UNODC) • The prosecution authorities received 265 MLA on tax crimes in 2015–2019, 100 of which are self-laundered ML-related	**Very high**	**Very high**	**Very high**
Corruption and bribery	• Estimated to generate about 2% of crime proceeds globally (UNODC) • Prosecution authorities received 100 MLA on corruption and bribery in 2015–2019, 63 of which are self-laundered ML-related	**High**	**Very high**	**Very high**
Drug trafficking	• Estimated to generate about 30% of crime proceeds globally (UNODC) • Luxembourg may be exposed to this threat externally both via financial flows from abroad, and due to its proximity with countries estimated to have sizable drug trafficking activity such as Germany, France, and the Netherlands given their market sizes • The prosecution authorities received 176 MLA on drug trafficking in 2015–2019, 44 of which are self-laundered ML-related	**High**	**High**	**High**

Predicate offence	Data/evidence summary	Likelihood/ probability	Size/ proceeds	Overall threat level
Participation in an organised criminal group & racketeering	• Organised crime (also including kidnapping, piracy, illicit arms trade) overall generates about 9% of crime proceeds globally (UNODC) • The prosecution authorities received 261 MLA on organised crime in 2015–2019[178]	**Medium**	**Very High**	**High**
Counterfeiting and piracy of products	• Acquisitive crime (incl. 6 LU predicate offences) overall generates 5–10% of crime proceeds globally (UNODC) • The prosecution authorities received 14 MLAs on counterfeiting and piracy of products in 2015–2019, of which 3 are self-laundered ML-related	**Medium**	**High**	**High**
Smuggling	• Acquisitive crime (incl. 6 LU predicate offences) overall generates 5–10% of crime proceeds globally (UNODC) • The prosecution authorities received 4 MLA on smuggling in 2015–2019	**Medium**	**High**	**High**
Sexual exploitation, including sexual exploitation of children	• Modern slavery overall generates about 2% of crime proceeds globally (UNODC) • The prosecution authorities received 173 MLAs on sexual exploitation in 2015–2019, of which 5 are self-laundered ML-related	**High**	**Medium**	**High**
Cybercrime	• The Prosecution authorities received 308 MLAs on cybercrime in 2015-2019, of which 31 are self-laundered ML-related	**High**	**Medium**	**High**
Illicit arms trafficking	• Organised crime (also including kidnapping, piracy, illicit arms trade) overall generates ~9% of crime proceeds globally (UNODC) • The prosecution authorities received 21 MLA on illicit arms trafficking in 2015–2019, of which 3 are self-laundered ML-related	**Medium**	**Medium**	**Medium**
Insider trading and market manipulation	• The prosecution authorities received 13 MLAs on insider trading in 2015–2019, of which 2 are self-laundered ML-related	**Medium**	**Medium**	**Medium**
Robbery or theft	• Acquisitive crime (incl. 6 LU predicate offences) overall generates 5–10% of crime proceeds globally (UNODC) • The prosecution authorities received 307 MLA on robbery or theft in 2015–2019, of which 22 are self-laundered ML-related	**Medium**	**Low**	**Medium**

[178] Note: The 261 MLAs for "participation in an organised criminal group & racketeering" also include other predicate offences, mostly Fraud. Only 10 MLAs only include "Participation in an organised criminal group & racketeering"

Predicate offence	Data/evidence summary	Likelihood/ probability	Size/ proceeds	Overall threat level
Trafficking in human beings and migrant smuggling	• Modern slavery overall generates about 2% of crime proceeds globally (UNODC) • The prosecution authorities received 11 MLA on human trafficking in 2015–2019 (none self-laundered ML-related)	**Low**	**Medium**	**Medium**
Illicit trafficking in stolen and other goods	• The prosecution authorities received 86 MLA on illicit trafficking in stolen or other goods in 2015-2019, of which 43 are self-laundered ML-related	**Low**	**Medium**	**Medium**
Environmental crimes	• Acquisitive crime (including 6 LU predicate offences) overall generates 5–10% of crime proceeds globally (UNODC) • The prosecution authorities received 2 MLA on environmental crimes in 2015–2019 (none self-laundered ML-related)	**Low**	**Low**	**Low**
Extortion	• Acquisitive crime (including 6 LU predicate offences) overall generates 5–10% of crime proceeds globally (UNODC) • The prosecution authorities received 88 MLA on extortion in 2015–2019, of which 5 are self-laundered ML-related	**Low**	**Low**	**Low**
Murder, grievous bodily injury	• The Prosecution authorities received 116 MLA on murder in 2015-2019, of which 1 is self-laundered ML-related	**Low**	**Low**	**Low**
Kidnapping, illegal restraint and hostage taking	• Organised crime (also including kidnapping, piracy, illicit arms trade) overall generates ~9% of crime proceeds globally (UNODC) • The prosecution authorities received 26 MLA on kidnapping in 2015–2019, of which 1 is self-laundered ML-related	**Low**	**Low**	**Low**
Counterfeiting currency	• Acquisitive crime (including 6 LU predicate offences) overall generates 5–10% of crime proceeds globally (UNODC) • The prosecution authorities received 10 MLA on counterfeiting currency in 2015–2019, of which 2 are self-laundered ML-related	**Low**	**Low**	**Low**
Piracy	• Organised crime (also including kidnapping, piracy, illicit arms trade) overall generates ~9% of crime proceeds globally (UNODC)	**Low**	**Low**	**Low**

5.2.2. Domestic exposure: Money laundering of proceeds of domestic crimes

The threat from money laundering of proceeds of domestic crimes is estimated to be smaller (overall moderate) than of foreign crimes. This is due to Luxembourg's low crime rate and limited presence of organised crime. The Organised Crime Portfolio[179] estimates that the aggregate revenue across a set of illicit markets (i.e. drug trafficking, fraud, counterfeiting, theft) in Luxembourg is around €161 million (i.e. ~0.4% of GDP), which is lower than for neighbouring countries (France: ~€16 billion or 0.8% of GDP; Germany: ~€17 billion or 0.7% of GDP; and Belgium: ~€2.5 billion or 0.7% of GDP), and close to half the estimate for the EU as a whole (i.e. 0.9% of GDP on average).

However, the Grand-Duchy's wealth, its economy, its high number of international institutions and its central location in Europe increase the threat level for certain crimes. Fraud and forgery, drug trafficking and robberies or theft emerge as the three most significant domestic threats. While some crimes might be perpetrated domestically, this does not necessarily imply that their proceeds are laundered domestically but might be taken abroad (e.g. offences committed by foreign organised crime groups, taking robbed goods or proceeds outside Luxembourg). Given the common market, criminals can easily cross the border to France, Germany or Belgium.

The table below provides an overview of threat levels and rationale for key domestic crimes.

[179] Organised Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

Table 11: Overview of threat levels, rationale for key domestic crimes

Predicate offence	Rationale	Likelihood/ probability	Size/ proceeds	Consequences/ impact	Overall threat level
Fraud and forgery	Fraud and forgery occur in many different forms LU's position as a payments, investment and cyber hub in Europe exposes it to higher proportion of fraud (applies to ML of both domestic and foreign proceeds) Relatively high occurrence of fraud in various forms (Police data: +4 000 cases per year)	High	High	High	High
Robbery and theft	Relatively high number of robberies and thefts in LU, of different goods; but proceeds likely to be sold/laundered abroad Relatively medium monetary loss/reputational impact	High	High	Medium	High
Drug trafficking	Generates €25–80 billion globally, and €9–20 million in LU LU consumption in line/slightly below world average Mostly domestic/retail usage rather than organised crime Finances organised crime and violence in LU and abroad	High	Low	High	Medium
Tax crimes	Globally the largest crime in terms of proceeds generated In LU, small shadow economy[1] & limited domestic tax evasion Reputational impact on LU if scandal emerges	Medium	Medium	Medium	Medium
Cybercrime	Luxembourg is ranked 11th country in the world for cybersecurity Agencies work hand in hand with Europol on cybercrime cases Impact of cybercrime can be significant impact on economy and individual lives	Low	Medium	High	Medium
Corruption and bribery	Low corruption in LU (i.e. limited proceeds for ML) High number of politically exposed persons (PEPs) in LU due to the presence of EU institutions (but still low in absolute number) Corruption erases trust in economic/political institutions	Low	Low	High	Medium
Participation in organised criminal groups	European OCGs operating in Luxembourg (for example France, Belgium and Eastern Europe) though with lower activity given small domestic market Robberies and theft as main activity of OCG (captured separately)	Low	Low	High	Medium
Sexual exploitation	Prostitution is not illegal in LU but procurement is Crime with major human consequences	Medium	Low	High	Medium

Predicate offence	Rationale	Likelihood/ probability	Size/ proceeds	Consequences/ impact	Overall threat level
Trafficking in human beings	EU common market (free movement of people) High number of migrants, refugees and asylum seekers relative to LU's size; but small in absolute numbers Modern slavery prevalence in LU amongst lowest globally	**Low**	**Low**	**High**	**Medium**
Extortion	Includes online extortion, with prominent cases in recent years Extortion only effective if carried out by organised crime; but no transnational racketeering groups identified in LU High human/social impact in case of widespread extortion	**Medium**	**Medium**	**Low**	**Medium**
Insider trading	Large financial centre, but limited trading activity (Luxembourg Stock Exchange) and low risk trading activity (bonds) Only a few small reported cases over the past years Distortion of competition/markets, plus reputational impact	**Low**	**Medium**	**Low**	**Low**
Counterfeiting and piracy	Proceeds in LU well below world average European logistics hub – could be transiting country for goods (such as counterfeited cigarettes and clothes) Indirect impact on IP rights and on local merchants	**Low**	**Very Low**	**Low**	**Low**

Table 12 provides an overview of key data points used in the assessment of domestic threat level per predicate offences (self-laundered ML), in the period 2017-2019 as per the sub-sections below. Note: The assessment looks at an aggregate across 2017-2019 to account for year-to-year volatility.

Table 12: Key data used in the assessment of domestic threat level per predicate offences, 2017-2019

	New notices (ML by predicate offence category), 2017–2019[180]		New prosecutions (ML by category), 2017–2019[181]		New sanctions (ML, by category), 2017–2019[182]		Domestic seizures, 2017–2019			
Predicate offence	Cases, # (of which ML)	Persons, # (of which ML)	Cases, # (of which ML)	Persons, # (of which ML)	Prison sentences[183], # (of which ML)	Suspended prison sentences[184], # (of which ML)	Total #[185] (of which ML)		Total volume, € million (of which ML)[186]	
Fraud and forgery	7 836 (388)	9 227 (1027)	1 321 (187)	2 010 (315)	158 (35)	298 (78)	53	(16)	~26.1	(~19.3)
Robbery and theft	49 581 (200)	20 453 (453)	3 433 (154)	4 002 (260)	714 (115)	484 (89)	49	(17)	~2.71	(~1.6)
Drug trafficking	1 099 (279)	1 992 (534)	552 (272)	906 (432)	205 (164)	421 (336)	92	(35)	~0.19	(~0.07)
Tax crimes	142 (14)	341 (35)	21 (3)	42 (13)	0 (0)	2 (0)	1		~1.1	
Cybercrime	703 (9)	345 (16)	16 (4)	20 (4)	0 (0)	0 (0)	2	(1)	~1	(~1)
Corruption and bribery	59 (3)	88 (13)	29 (4)	36 (7)	1 (0)	9 (0)	3	(3)	~65.8	(~65.8)
Participation in organised criminal groups	139 (33)	453 (160)	55 (21)	153 (55)	15 (9)	17 (7)	7	(6)	~1.1	(~1.1)
Sexual exploitation	371 (5)	456 (6)	103 (5)	122 (10)	11 (2)	78 (5)	0		-	
Trafficking in human beings	201 (14)	428 (62)	8 (1)	15 (3)	2 (1)	18 (5)	1	(1)	-	
Insider trading	5 (0)	11 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0		-	
Counterfeiting and piracy	24 (2)	44 (4)	5 (1)	11 (2)	0 (0)	1 (0)	1		-	
Illicit trafficking in stolen and other goods	627 (125)	1 038 (300)	213 (63)	379 (107)	30 (13)	25 (14)	10	(8)	~4.81	(~4.80)
Murder, grievous bodily injury	1 580 (1)	2 126 (3)	447 (4)	575 (7)	25 (1)	96 (0)	2		~1.3	

[180] Parquet Général Statistical Service, data received in August/September 2020
[181] Parquet Général Statistical Service, data received in August/September 2020
[182] Parquet Général Statistical Service, data received in August/September 2020
[183] Sans sursis.
[184] Sursis partiel, sursis total.
[185] Parquet Général Statistical Service, data received in April 2020
[186] For both total and SL ML volume of domestic seizures, Parquet Général Statistical Service, data received in August 2020

	New notices (ML by predicate offence category), 2017–2019[180]		New prosecutions (ML by category), 2017–2019[181]		New sanctions (ML, by category), 2017–2019[182]		Domestic seizures, 2017–2019	
Extortion	457 (9)	427 (22)	61 (4)	132 (11)	15 (2)	15 (5)	3 (1)	-

The sub-sections below provide an overview of the overall threat level across all domestic predicate offences.

5.2.2.1. Fraud and forgery

Fraud and forgery constitute a significant ML threat for Luxembourg. The probability and proceeds of crime are high, considering the broad range of offences within the scope of fraud and forgery[187], and the high figures reported by the Grand-Ducal Police, the prosecution authorities and the CRF.

Fraud and forgery are one of the most important domestic predicate offences, after drug trafficking and robberies/theft. In 2018, the Grand-Ducal Police[188] reported 1366 "other criminal offences against goods"[189], a category which includes "breaches of trust"[190], "fraud/trickery"[191], "financial crime"[192] and "forgery or falsification"[193] amongst others. It should be noted that these figures stem from the crimes reported by the general population to the Grand-Ducal Police and do not necessarily include cases treated by the specialised units within the Grand-Ducal Police, which explicitly deal with financial and economic crime, including ML.

In 2017-2019, 7 836 fraud and forgery cases have been opened, of which 388 potential ML cases identified for investigation. These cases concerned 9 227 suspects (of which 1 027 related to potential ML). During the same period, 1 321 cases were prosecuted (of which 187 potential ML), concerning 2 010 persons (of which 315 to potential ML). These resulted in 158 prison sentences (of which 35 for ML), and 53 seizures for a total amount of €26.1 million (of which 16 for a total amount of €19.3 million related to ML[194]).

As highlighted above, Luxembourg's position as a payment, investment and cyber hub increases the likelihood that criminals (in Luxembourg and abroad) commit fraud involving Luxembourg-based institutions (wittingly or unwittingly), and potentially launder the proceeds of that fraud via Luxembourg.

The ECB reports that 74% of EU e-money transactions have been made in Luxembourg in 2018[195], reflecting the fact that PayPal and Amazon Payments have established their European headquarters in the country. Moreover, 97 wealth and asset managers with €40.6 billion assets under management (AuM) have established themselves in the country[196], with numerous clients, substantial international business (55.9% of AuM are from international business) and foreign ownership (41% of firms are foreign-owned). While it is difficult to determine the proportion of fraudsters based in Luxembourg that launder their proceeds domestically, it is likely that some of the proceeds would fall under the scope of domestic ML exposure.

[187] Fraud against government (including VAT fraud); embezzlement/misappropriation; lending fraud; payment fraud; insurance fraud; healthcare fraud; benefit fraud; vendor, supplier & procurement fraud; confidence tricks/scams; false billing/invoicing; cyber & Internet selling fraud; investment fraud; forgery of financial assets; philatelic forgery; fake passports, drivers licenses and IDs; fake art; illegal gambling.

[188] Grand-Ducal Police Annual Report 2018 (link)

[189] "Autres infractions contre les biens"

[190] "Abus de confiance"

[191] "Escroqueries/trumperies"

[192] "Délits financiers"

[193] "Contrefaçons et falsifications"

[194] Data received from Parquet Général Statistical Service in August/September 2020

[195] ECB, Payment Statistics (full report); Table 7.1 Number of payments per type of payment service, 2018 figures (link)

[196] CSSF data provided for Sectorial vulnerabilities of the NRA in 2020

Reported proceeds generated by fraud and forgery, as well as the complexity of the offence, are considerable). In 2019, the CRF has transmitted 156 analysis products to the prosecution authorities for fraud and forgery (out of a total of 219 analysis products across all predicate offences)[197].

Finally, the economic consequences of fraud and forgery could be material for Luxembourg. Fraud events (e.g. investment scandals) could erode trust in the Grand-Duchy and expose financial institutions and tech companies to reputational risk. Furthermore, fraud and forgery impose direct economic losses to both victims and the government.

The typology below illustrates an example of fraud attempt in a private bank through an external advisory.

Case Study 9: Investment scam to convince private banking clients to invest in illicit schemes

A fraudulent advisor contacts a client of a private bank. The fraudster claims that he/she has been appointed as nominee settlor of a trust of which the potential victim is the beneficiary.

The fraudulent advisor acknowledges the numerous scams on the internet and offers to meet the potential victim in person.

The fraudulent advisor assures the potential victim that no up-front fee payment is to be made and that fees, if any, would be deducted directly from the amount to be disbursed to the potential victim.

The fraudulent advisor sends the potential victim an authentic-looking trust deed and disbursement notice in the targeted clients' name. The trust deed seems to be certified by a notary. The disbursement notice bears the name and signature of an employee who recently left.

As described in the external exposure section, fraud and forgery have been noted by both domestic and international bodies as a growing threat in the context of the COVID-19 pandemic[198].

5.2.2.2. Robbery or theft

Domestic robberies and thefts are a relevant threat for Luxembourg. The number of offences per capita is higher than in peer countries and the proceeds are believed to be high on aggregate relative to other crimes.

[197] It should be noted not all files transmitted to the prosecution authorities from CRF necessarily result in new notices (prosecution authorities might not process all transmission in a given year, and/or decide not to open an investigation based on transmissions received). Additionally, as explained in the CRF section, in 2017 it increased its selectiveness by doing additional analysis and "triage" ahead of transmitting files to the prosecution authorities, only transmitting files it already deems to have a high likelihood of being prosecuted. It is estimated that a high proportion of fraud cases transmitted from the CRF to the prosecution authorities prior to 2017 actually relate to "attempted fraud" cases, which banks are required to report to the CRF via an STR.

[198] See, for instance, CSSF, *Circular 20/740*, 2020 (link); EUROPOL, *Pandemic profiteering – How criminals exploit the COVID-19 crisis*, 2020 (link); and FATF, *COVID-19-related Money Laundering and Terrorist Financing* (link)

Robberies and thefts are the most important domestic predicate offence in Luxembourg across a broad range of statistics, more prevalent than in peer countries. The Grand-Ducal Police[199] reported 2 568 thefts related to vehicles, 3 667 house break-ins and burglaries[200] and 10 422 other thefts in 2018. While high, the number of offences and attempts has remained stable since 2013. In 2017–19, the prosecution authorities opened 49 581 new notices implicating 20 453 persons (of which 200 new cases implicating 453 persons for potential ML). During the same period, the prosecution authorities decided to prosecute 3 433 cases implicating 4 002 persons (of which 154 ML cases implicating 260 persons), leading to 714 prison sentences (of which 115 for ML)[201]. Eurostat figures support that there are more robberies, thefts and burglaries per capita in Luxembourg than in other European countries (22.8 per 1 000 residents vs. 19.9 EU average)[202].

Foreign organised criminal groups and individual criminals are believed to target Luxembourg due to its wealth and proximity to three borders. In fact, Luxembourg has the highest GDP per capita in the EU, over 2.5 times the EU average in 2018[203]. Judiciary authorities note an impression of easy escape from crime scenes, by way of the Grand Duchy's proximity to the French, Belgian and German borders. Based on experience from the prosecution authorities and the police, foreign perpetrators targeting Luxembourg for robberies and thefts come from a variety of locations, including the border region, but also Eastern Europe. Crimes have targeted a wide range of goods, including cars, bicycles, jewellery, hospital equipment and construction site materials. For example, the Organised Crime Portfolio estimates cargo theft revenues in Luxembourg of €1.9 million[204], which is higher in absolute terms than the estimates for Portugal, Ireland or Greece.

Given that stolen goods are frequently transported abroad for resale (as commonly proceeds of crimes are moved from where they were perpetrated), it is estimated the proceeds for money laundering usually do not remain in Luxembourg. This is reflected in the relatively low number of transmissions to the prosecution authorities and asset seizures. In 2019 the CRF has transmitted 3 analysis products to the prosecution authorities for robberies or theft (out of a total of 219 analysis products across all predicate offences)[205]. Furthermore, the prosecution authorities seized money-laundered assets for domestic crimes worth roughly €2.7 million in 2017–2019.

The consequences of robberies and theft mostly relate to the monetary loss of the items. While physical and emotional harm is difficult to assess, it is believed to be limited. Robberies and thefts can be accompanied by some violence; the Grand-Ducal Police reported 412 thefts with violence in 2018[206]. Moreover, robberies and theft are likely to contribute to a feeling of insecurity among the population.

5.2.2.3. Drug trafficking

While the size of proceeds is low relative to other threats, the use of drugs is average compared to other countries, and the human and social impact are high.

Europol[207] estimates drug sales in Luxembourg to constitute less than 0.1% of GDP. Drug consumption in Luxembourg is broadly in line with world average. According to UNODC, ecstasy consumption

[199] Grand Ducal Police Annual Report 2018 (link)
[200] This figure relates to any attempt or offence of a break-in to a property, whether or not it involved theft of property.
[201] Data received from Parquet Général Statistical Service in August/September 2020
[202] Eurostat, *Crime and criminal justice tables*, 2017 (link)
[203] Eurostat, GDP per capita, consumption per capita and price level indices (link)
[204] Organized Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)
[205] CRF Annual Report, 2018
[206] Grand Ducal Police Annual Report 2019 (link)
[207] Eurostat database (link)

(0.48%) is in line with the world average (0.50%), while cannabis consumption is slightly above (5.20% with a world average of 4.47%)[208].

Drug trafficking in Luxembourg is mostly based on "street dealing" of drugs imported from neighbouring countries rather than large organised crime groups importing or producing drugs for local resale. Most offences recorded are on possession and use of drugs vs. trafficking. Crime level is broadly in line with neighbouring countries. The Grand-Ducal Police reported 4 238 drug offences and attempts[209] in 2017 (12% of all offences registered, vs. 7% in Ireland[210] and 17% in Belgium[211]), down from 4 675 drug offences and attempts in 2015 (20% of all offences and attempts registered). In 2017–19, the prosecution authorities opened 1 099 drug trafficking cases for investigation (of which 279 potential ML cases) related to 1 992 persons (of which 534 for potential ML). In the same period, the prosecution authorities decided to prosecute 552 cases (of which 272 cases for ML) implicating 906 persons (of which 432 persons for ML), leading to 205 prison sentences (of which 164 for ML)[212].

While the domestic proceeds of crime generated in Luxembourg are estimated to be lower than in other jurisdictions, the levels of criminal proceeds and the adjacency to countries with high levels of proceeds raise the level of ML threat. The proceeds generated by drug trafficking in Luxembourg are estimated between €9 million[213] and 20 million[214] annually (representing ~€30 per resident annually); this is lower than estimated proceeds of €28 billion[215] to €80 billion[216] annually in Europe (representing ~€55 per resident annually[217]). The CRF transmitted three drug trafficking cases to the prosecution authorities in 2019, and recorded 1 572 SARs and STRs for drug trafficking in 2019[218]. In 2017-2019, the prosecution authorities seized ~€0.2 million from domestic drug trafficking cases of which €66 400 were money laundering related. It is however becoming increasingly difficult to detect amounts generated by drug trafficking with the emergence of new drug trafficking methods (e.g. Dark Web platforms). Luxembourg's central location and its increasing role in logistics[219] may also pose a threat, as it is possible that some drug-trafficking may be transited through Luxembourg. While proceeds of domestic drug dealing are likely to be laundered domestically and in neighbouring countries (due to the street-dealing nature of trafficking), proceeds from drugs transiting through Luxembourg (an organised crime activity) are probable to be laundered abroad.

Drug trafficking results in significant human and social cost. Drug trafficking leads to addiction and death, and finances organised crime. The Luxembourg Institute of Health reported 5 846 "problematic registered drug users" (~1% of the population) and five deaths in 2016 (0.9 deaths per 100 000 people aged 15–64, down from 5.9 in 2000).[220] This is slightly below the European average of 2.3 (with a total

[208] UNODC statistics database, *Drug Use and Health Consequences, Annual prevalence for adults (15-64 years old) for "Ecstasy Type Substances" and "Cannabis"* (Luxembourg data as of 2010) (link)

[209] Grand Ducal Police Annual Report 2019 (link)

[210] Ireland, *National Risk Assessment for Ireland, Money Laundering and Terrorist Financing*, 2015 (link)

[211] Federal Police Belgium, Annual Report 2017 (link)

[212] Data received from Parquet Général Statistical Service in August/September 2020

[213] Organized Crime Portfolio, *Illicit Revenues and Criminal Investments in Europe*, 2015 (link)

[214] STATEC, *Regards sur l'impact de l'économie illégale sur l'économie luxembourgeoise*, 2014 (link)

[215] Organized Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

[216] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011 (link)

[217] ~€55 per resident using the OCP estimates for total EU (€28 BN); the OCP study estimates proceeds of ~€7 billion in Luxembourg's 3 neighbouring countries (France, Germany, Belgium), which represents ~€44 per resident

[218] Note cases transmitted by the CRF to the prosecution authorities, as well as STRs, can relate to domestic ML and foreign ML; note also the annual estimates for drug trafficking proceeds referred in the previous paragraph are estimates based on annual average data from cited sources, and not the estimate for a specific year.

[219] Luxembourg Trade & Invest, *Logistics Hub Luxembourg*, 2017 (link)

[220] Luxembourg Institute of Health, *National Drug Report*, 2017 (link)

of 7 585 drug-induced deaths in Europe in 2017[221]). Finally, combating drug trafficking is a key focus of domestic law enforcement authorities with significant resources allocated to this offence.

5.2.2.4. Tax crimes

While domestic tax crimes occur in Luxembourg, the threat is considered less significant than for other countries, due to the Grand-Duchy's tax system, its small shadow economy[222], and limited number of recorded offences.

Local businesses and individuals tend to pay their taxes thanks to a tax regime that is not complex, easy to use and relatively low corporate taxes. The Grand-Duchy is ranked 21 out of 190 countries for the complexity of its tax regime[223]: the average company pays the lowest tax and contribution rate in the EU (20.5% vs. 39.6% average) and takes the third lowest time to comply with tax obligations in the EU (55 hours vs 161 hours average). The World Economic Forum Global Competitiveness Index also assesses that Luxembourg ranks fourth out of 137 countries for less distortive effect of taxes and subsidies on competition[224]. In recent years Luxembourg joined a series of international agreements and exchanges of tax information initiatives[225]. For example, the Grand-Duchy has introduced legislation to implement the OECD's Common Reporting Standard (CRS) for the automatic exchange of financial information. Luxembourg is also actively involved in the OECD Base Erosion and Profit Shifting (BEPS) initiative and has enacted legislation to address BEPS 13, on country-by-country reporting. Automatic sharing of information is expected to contribute significantly to *ex-ante* prevention and lower cases on tax offences being transmitted to the prosecution authorities (and/or being object of LAR).

Data from Luxembourg's direct tax administration shows overall stable tax revenue, with manageable amounts outstanding to be collected (which generate associated interest and other costs for late payers) and sanctions for late payment in given circumstances. Overall direct tax revenue (€10.6 billion in 2019) is roughly split amongst individuals (~58%, ~€5.9 billion) and legal persons (~42%, ~€7.4 billion)[226]. For individuals, 94% of the 2019 workforce of 443 718 persons ("emploi salarié intérieur")[227] are employed (*"salariés"*). Taxes on salaries are collected throughout the year via withholding with employers ("*retenue d'impôt sur les traitements et salaires")* which further contributes to reduce the likelihood of fraud or evasion.

Across both individuals and legal persons, taxes outstanding (to be collected; "*solde général*") amounted to about €1.7 billion as of December 2019, of which 17.8% of these concerned taxes were not yet due or still within the legal time limits and/or acceptable time limits to ACD, 57.9% was effectively categorised as "due" and only 24.3% was categorised as "being enforced" ("*soumis à contrainte*"). Late payers can be subject to paying interest on late payments[228] (€26 million in 2019), as well as fines and sanctions for late/non-payment[229] (€9.9 million in 2017). In 2016–2017, Luxembourg ran a 2-year fiscal "*régularisation*" allowing taxpayers to voluntary disclose complete and corrective tax returns, in exchange for exemption from prosecution for tax crimes on the basis of the corrective filings submitted and payment of an additional surcharge. This resulted in additional

[221] European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *Statistical Bulletin 2017 — overdose deaths* (link)
[222] Illicit economic activity existing alongside a country's official economy, e.g. black market transactions and undeclared work.
[223] PWC & World Bank, *Paying Taxes,* 2018 (link)
[224] World Economic Forum, *The Global Competitiveness Index*, 2019 (link)
[225] Further details can be found in the Detection (ACD) section
[226] Data provided by ACD in June 2020
[227] STATEC, Emploi, chômage et taux de chômage par mois (données désaisonnalisées) 1995-2020.
[228] *Intérêts de retard,* data provided by ACD in June 2020
[229] *Amendes, astreintes et recettes analogues* (including "*majoration*" from the fiscal "*régularisation*"); ACD data.

revenue of ~€54.5 million (~1% of total tax revenue for individual persons, or 0.6% of total tax revenue).[230]

Luxembourg's (estimated) small shadow economy is also believed to contribute to a more limited domestic threat of tax crimes, also supported by low number of domestic offences. In fact, the Institute for Economic Affairs estimates that the shadow economy represents ~10% of national income (in line with Switzerland, but significantly below the world average of 33%)[231]. This explains why domestic tax evasion (0.9% of GDP) is estimated lower than for most other 38 OECD countries[232] (e.g. 1% to 1.1% in Germany, France and Belgium). In 2017–2019, the prosecution authorities opened 142 tax offence new cases for investigation (of which 14 potential ML cases). These cases concerned 341 suspects of which 35 related to potential ML. The prosecution authorities decided to prosecute 21 cases, implicating 42 persons (3 cases implicating 13 persons for ML). Over the same time, there were no convictions for ML proceeds of tax crimes[233]. It should be noted that Luxembourg has added aggravated tax evasion and tax fraud to the list of predicate offences for ML as of January 2017[234], helping to reduce the likelihood of crime.

While historically lower than in other countries, proceeds of domestic tax evasion are still significant, with tax crime is estimated to be one of the most common offences in most countries (estimates suggest it may represent as much as 30% of the world crime proceeds[235]). The prosecution authorities seized assets from domestic tax evasion cases of ~€1.1 million in 2017–2019[236]. Proceeds of domestic tax evasion are likely to be laundered both domestically (e.g. through cash payments for shadow economy activities and retail purchases) and abroad.

Importantly, tax-related scandals are a sensitive issue for Luxembourg due to its significant financial centre. On 14 May 2020, the European Commission launched legal actions against Luxembourg over laws to prevent money laundering and tax avoidance. Along with more than half of the EU member states, Luxembourg is being accused of not having adopted new EU rules which became operational this year[237]. This increased scrutiny may result in reputational consequences for Luxembourg, particularly given its financial stature.

It should also be noted, domestic tax evasion may represent an opportunity cost of lost tax revenues to the state and the consequent impact of public services not financed.

5.2.2.5. Cybercrime

Cybercrime is considered a significant threat for Luxembourg. While the likelihood is low, given a significant investment in cybersecurity, rendering the country 11th in the world for cybersecurity[238], potential data breaches can have major consequences on data protection, confidentiality and availability, with important social and economic costs.

---

[230] Based on a total of ~€8.5 billion total direct tax collected, of which ~€5 billion on natural persons. All data points in data pack provided by ACD on 04/07/2018.

[231] Institute for Economic Affairs, *The Shadow Economy*, 2013 (link)

[232] CESifo Group, *Size and Development of Tax Evasion in 38 OECD Countries*, 2012 (link)

[233] Data received from Parquet Général Statistical Service in August/September 2020

[234] While aggravated tax evasion has been added as a new offense, tax fraud was already criminalised prior to 2017. With the Law of 23 December 2016 implementing the 2017 tax reform, the legislation has been strengthened and both offences are now also a predicate offence to ML. See section on Prosecution for further details, including the laws criminalising tax crimes

[235] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011 (link)

[236] Data received from Parquet Général Statistical Service in August 2020

[237] Reuters, May 2020 (link)

[238] ITU 2019, Global Cybersecurity Index, based on legal, technical, organisation, capacity building and cooperation pillars

Public and private actors have significantly invested in Luxembourg's cyber infrastructure and connectivity, building an important information network that connects Luxembourg to the main European hubs of the numerical economy. Alongside this investment, Luxembourg developed a rising consciousness of associated risks. As such, a national cybersecurity strategy was developed in 2012, updated in 2015 and again in 2018. Alongside the strategy, a Cybersecurity Board and Cybersecurity Competence Centre was set up within the government. Furthermore, Luxembourg has made cybersecurity-related research a national priority, with 250 researchers specialising in the field, at the Interdisciplinary Centre for Security, Reliability and Trust at the University of Luxembourg. Luxembourg's Service de Police Judiciaire has a separate cybercrime unit, specifically working on cybercrime cases, in close collaboration with other units, including economic and financial crime, and drug trafficking, given the close association of cybercrime to other types of crime. It should also be noted that the unit cooperates with Europol.

In 2019, CRF reported 517 cybercrime STRs, and ordered freezing procedures in three cases for a total amount of €65 607.61. The CRF transmitted seven files to prosecution authorities in 2019. In 2017-2019 the prosecution authorities opened 703 new cases (of which 9 for potential ML) for investigation, implicating 345 suspects (of which 16 for potential ML). In the same period, the prosecution authorities decided to prosecute 16 cases (of which 4 for ML), implicating 20 persons (of which 4 for ML). While the number of suspected activities is low versus other risks, potential data breaches have major consequences on data protection, confidentiality and availability. The use of data illicitly obtained (such as passwords) can cause significant human harm, including identity theft. Furthermore, the use of ransomware can have significant impact on the economy, for example by resulting in shutting down core systems of banks and hospitals.

Importantly, cybercrime and the risks associated with cybersecurity have increased since the outbreak of the COVID-19 pandemic and the imposition of lockdown measures driving demand for communication, information and supplies through online channels. Criminals use phishing and ransomware campaigns (such as those included in the case studies below) to exploit the current crisis and capitalize on the anxieties and fears of their victims[239]. CRF's COVID-19 typologies report highlights that working from home creates new risks, as criminals can exploit security loopholes to gain confidential documents, which are then used in sophisticated frauds[240]. Further detail is provided in section 4 of the NRA on the impacts of COVID-19.

5.2.2.6. Corruption and bribery

The level of domestic criminality is deemed to be relatively low in Luxembourg. Transparency International ranks the country ninth out of 180 in its Corruption Perception Index[241] (alongside Germany), and the World Bank ranks Luxembourg in the top 3% worldwide in its Controls of Corruption Index[242]. Moreover, the 1997 OECD Anti-Bribery Convention, the 1999 Council of Europe Criminal law convention on corruption (STE no. 173), the 2000 UN Convention on transnational organised crime and the 2003 UN Convention against corruption have all been implemented into national law between 2001 and 2007.

The proceeds of corruption and bribery generated in Luxembourg are also deemed low. In fact, the prosecution authorities recorded just three seizures of a domestic corruption case in 2017–19. The CRF transmitted three files to the prosecution authorities in 2019. The Grand-Duchy has an overall small sized economy, making corruption in public procurement contracts possibly less attractive (e.g.

[239] EUROPOL, *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic,* 2020 (link)
[240] CRF, *Typologies COVID-19*, 2020 (link)
[241] Transparency International, *Corruption Perception Index*, 2019 (link)
[242] World Bank, *Data Bank: Worldwide Governance Indicators, Control of Corruption*, 2018 (link)

public spending of 42% of GDP in 2017[243]). Luxembourg is also not a large receiver of EU funds: in 2018, it was the 18th largest receiver out of EU28 with €2 billion[244]. Together with observed high transparency, this supports why only 16 offences and attempts of misuse of (public) funds were reported by the general population to the Grand-Ducal Police in 2016–17[245]. Perpetrators are also more likely to be individuals rather than organized crime groups. In the 2017-2019 period, 59 corruption and bribery cases have been opened, of which 3 potential ML cases identified for investigation. These cases concern 88 suspects of which 13 related to potential ML. During the same period, prosecution authorities decided to prosecute 29 cases (including 4 for ML) related to 36 persons (including 7 for ML).

However, the significant presence of international organisations in Luxembourg[246] and its role in the domestic economy increases the exposure to this type of crime, with significant social and reputational costs. Corruption shown in public indices and in prosecution authorities/CRF figures as described above mostly captures traditional low-level corruption. The high number of PEPs residing or working in Luxembourg (e.g. those working in European institutions or other multilateral organizations based in the country) could be abused or misused for ML and increase the threat level. Such events would reduce confidence in EU institutions and would also have major reputational impacts for the country. Corruption could lead to erosion of trust in economic and political institutions and would increase the cost of doing business[247]. Moreover, multilateral and other international organizations based in Luxembourg (which drive the number of PEPs residing or working locally) could spread this impact significantly beyond Luxembourg.

As noted in the external exposure section, corruption and bribery have been noted as growing threats in the context of the COVID-19 pandemic, particularly in relation to government support schemes. Further detail is provided in section 4 of the NRA on the impacts of COVID-19.

5.2.2.7. Participation in organised criminal group and racketeering

The domestic level of organised crime is deemed to be relatively low in Luxembourg. None of the main criminal groups in Europe have been estimated to operate in Luxembourg[248]. Nonetheless, judiciary authorities report that organised crime groups sometimes target the Grand-Duchy, especially for robberies, thefts and burglaries. Considering that the Luxembourg market is relatively small however, the likelihood of crime can be assessed to be relatively low. This is in line with numbers from the prosecution authorities. In 2017-2019, 139 cases have been opened, of which 33 potential ML cases identified for investigation These concern 453 suspects, of which 160 for potential ML. In the same period, the prosecution authorities decided to prosecute 55 cases (of which 21 related to potential ML), implicating 153 suspects, (of which 55 related to potential ML). While organised crime only has a limited presence in Luxembourg, it may promote violence, social disruption and increased cost of living.

Proceeds of organised crime in Luxembourg are difficult to estimate but could be relatively more significant. UNODC estimates organised crime to generate 9% of world crime proceeds[249] – in Luxembourg this figure is likely to be much lower. In 2017-2019, the prosecution authorities recorded

[243] OECD, *General government spending, Total, % of GDP*, 2017 (link)

[244] European Commission, *EU expenditure and revenue 2014-2020* (2016 total expenditure) (link)

[245] Grand Ducal Police Annual Report 2017 (link); "*détournements*"

[246] See for example: The official portal of the Grand-Duchy of Luxembourg, *Luxembourg, seat of European institutions* (link)

[247] World Economic Forum, *Global Agenda-Council on Anti-Corruption*, 2012

[248] Organized Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

[249] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, 2011 (link)

~€1.1 million seizures for domestic cases. The CRF has only transmitted two files to the prosecution authorities in 2019.

5.2.2.8. Counterfeiting and piracy of products

Luxembourg's role as an important logistics hub in the EU exposes[250] it to counterfeited products passing through. The country has the sixth largest airfreight platform in Europe, a freeport, significant rail freight, a multimodal terminal in Bettembourg/Dudelange, a logistics park and a high number of lorry drivers passing through the country each day. Judiciary authorities report that some counterfeited goods in transit have been seized (e.g. counterfeited cigarettes from Eastern Europe and counterfeited clothes from South East Asia. The prosecution authorities state that it is often difficult to identify individuals behind those crimes. This is reflected in the low numbers reported by prosecution authorities (i.e. 24 new cases for investigation in 2017–2019, of which 2 of potential ML, implicating 44 people, of which 4 suspects of potential ML, and 11 people prosecuted, of which two for ML over the same time).

The proceeds of counterfeiting and piracy of products are important based on available data: For instance, one study estimates the crime to generate about €42 billion in the EU annually[251]; another attributes ~$10 billion to the commercial value of unlicensed software in the EU[252], which is one type of product counterfeiting/piracy. In Luxembourg, counterfeiting revenues are also important (€63 million annually, ~0.1% of GDP) but below the world average (0.3%)[253]. Software piracy in Luxembourg is also less prevalent than in other countries: The commercial value of unlicensed software in use is estimated to be $20 million in 2017, which represents a share of unlicensed software over total software used at 17% compared to 37% global average[254]. Flows of proceeds are a mix of cash, physical and financial flows. Although the number of STR (two) and SAR (seven) reported by the CRF in 2019 is low, there were many electronic STR (6 336) and electronic SAR (377) filed by reporting entities active in an online environment. Prosecution authorities reported one seizure in 2017–2019 for domestic crimes of counterfeiting.

The economic and social consequences are important. Counterfeiting and piracy of products has an indirect impact on intellectual property rights, which are of fundamental importance for an advanced and innovative economy. Moreover, local merchants (e.g. clothes retailers) might suffer from lost revenues and the government loses on tax revenues as a result. Globally, counterfeit goods may also be linked to (child) labour exploitation. Some counterfeit products (in particular counterfeit medicine) entail health and safety risks for consumers, due to the often times inferior quality.

Counterfeiting and piracy have been noted as growing threats in the context of the COVID-19 pandemic, particularly in relation to medicines and other goods. Further detail is provided in section 4 of the NRA on the impacts of COVID-19.

5.2.2.9. Sexual exploitation, including sexual exploitation of children

The prevalence of prostitution and the relatively high number of reported domestic offences indicate that the probability of this crime is not negligible. Prostitution in the Grand-Duchy is not illegal, but

[250] Luxembourg Trade & Invest, *Logistics Hub Luxembourg*, 2017 (link)

[251] Organized Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

[252] BSA The Software Alliance, *BSA Global Software Survey*, 2018 (link)

[253] Organized Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

[254] BSA The Software Alliance, *BSA Global Software Survey*, 2018 (link)

procuring is, as are those activities associated with organised prostitution, such as profiting from (operating brothels and prostitution rings) or aiding prostitution. Furthermore, exploiting people in distress by paying them for sex is illegal. One study provides estimates of 300 to 5000 prostitutes in Luxembourg[255]. Another report, by the Ministry of Equal Opportunities estimates that there are ~50 active prostitutes per day in Luxembourg[256]. In 2017-2019, the prosecution authorities opened 371 new cases, of which 5 potential ML identified for investigation. These cases concerned 456 suspects, of which 6 related to potential ML. The prosecution authorities decided to prosecute 103 cases, of which 5 related to ML, implicating 122 suspects, of which 10 of ML. Over the same time, 11 prison sentences related to this predicate offence were pronounced, of which 2 related to ML[257].

However, the proceeds generated by sexual exploitation domestically are low. STATEC estimates prostitution to contribute to 0.21% of domestic production value in 2012, with annual proceeds of ~€80 million[258]. While this is significantly higher than for example drug trafficking (0.02%), not all elements associated with prostitution are illegal (see above). The prosecution authorities recorded no seizures for domestic cases in 2017-2019. Nonetheless, the Organized Crime Portfolio[259] estimates that human trafficking (including sexual exploitation but also removal of organs, forced labour and slavery) generates €36 billion in Europe annually, with France and Italy being the largest markets. Proceeds from activities associated with organised prostitution are likely to be laundered both domestically and abroad.

Still, sexual exploitation has a high economic and social cost, with victims subjected to long-lasting physical and emotional impact. It can also have some impact on the attractiveness for business due to the nature of the crime and broader concerns around labour exploitation and modern slavery associated with this offence. This topic is also a focus of cooperation with foreign counterparts from the Luxembourg's FIU, the CRF.

5.2.2.10. Trafficking in human beings and migrant smuggling

Luxembourg is in the centre of the EU common market, with its free movement of people, and has welcomed a high number of migrants, refugees and asylum seekers relative to its size. In fact, 48% of the local population are foreigners and 7% come from outside the EU[260]. Luxembourg has the fourth highest number of first-time asylum applicants per million habitants in the EU (915 vs. 2 725 in Malta and 383 EU average[261]). In the fourth quarter of 2019, 560 migrants in absolute terms have requested asylum status in Luxembourg, with most asylum seekers being from Syria (110), Eritrea (110) and Afghanistan (110). Local authorities have taken 2 154 decisions that year and given asylum status to 653 people (vs. 994 in 2018 and 1 176 in 2017)[262]. However, while Luxembourg is a very open economy, it is not a primary destination for human and migrant trafficking, considering its small size (e.g. only 0.3% of the 171 325 asylum applicants in the EU in the fourth quarter 2019 have applied in Luxembourg[263]); and Luxembourg is one of the countries with the lowest estimated prevalence of modern slavery by the proportion of their population (0.02% alongside Ireland, Norway and Switzerland[264]). This is in line with the low number of new cases in the 2017-2019 period: 201 cases

[255] P. Adair, O. Nezhyvenko, *Sex work vs. sexual exploitation: assessing guesstimates for prostitution in the European Union*, 2016 (link)

[256] Ministere de l'Egalite des chances, Rapport Platforme "Prostitution", 2014 (link)

[257] Data received from Parquet Général Statistical Service in August/September 2020

[258] STATEC, *Regards sur l'impact de l'économie illégale sur l'économie luxembourgeoise*, 2014 (link)

[259] Organized Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

[260] STATEC, *Le Luxembourg en chiffres*, 2019 (link)

[261] Eurostat Asylum Quarterly Report, Q4 2019 (link)

[262] MAEE, *Bilan de l'année 2019 en matière d'asile et d'immigration* (link)

[263] Eurostat Asylum Quarterly Report, Q4 2019 (link)

[264] Walk Free Foundation, *Global Slavery Index*, 2016 (link)

opened for investigation, of which 14 for potential ML, implicating 428 persons, of which 62 for potential ML. Over the same period, the prosecution authorities decided to initiate eight prosecutions, of which one for ML, implicating 15 persons, of which three for ML. Two prison sentences were pronounced, of which one related to ML.

Nonetheless, human trafficking in Europe generates significant proceeds (€36 billion in Europe each year as referred above – with Italy and France being the largest markets[265]), but available data suggests that Luxembourg is impacted to a lesser degree. The prosecution authorities recorded one seizure for domestic cases in 2019, of €240. Similarly, the CRF transmitted no files to the prosecution authorities in 2019, and reported nine STR in 2019. Given that human trafficking is mostly carried out by organised crime groups (which have limited presence in Luxembourg and where found, are foreign organised groups), proceeds are likely to be laundered abroad.

Finally, trafficking in human beings and migrant smuggling generates significant social and human harm, with particularly acute consequences for women and children. Moreover, there is a public expectation that financial institutions and governments have a role in preventing this crime and helping vulnerable persons where possible.

5.2.2.11. Extortion

Extortion is believed to be mostly effective when carried out by well-rooted organised crime groups[266], but no transnational racketeering groups have been identified in Luxembourg[267]. Overall, few cases have been reported in Luxembourg and since 2016, and the number of reported criminal offences and convictions has remained relatively stable. However, the human and social impact of such cases are significant, and notwithstanding the low number of cases, a few significant cases of online extortion in recent years have driven the overall threat level in Luxembourg up.

According to the Computer Incident Response Centre Luxembourg (CIRCL), a government-driven initiative providing a systematic response facility to computer security threats and incidents, an increasing number of attempted online scams since 2018[268]. In 2019, the CRF reported virtual assets directly related to extortion cases amounting to ~40 BTC, equivalent to ~€260 000, with a further ~3 230 BTC indirectly (or potentially) related[269], equivalent to ~€2 million[270].

The prosecution authorities have opened 457 new cases in 2017-2019 (of which 9 for potential ML), involving 427 people (of which 22 for potential ML). In the same period, 61 cases have been prosecuted (of which 4 for ML), involving 132 suspects (of which 11 for ML) and 15 prison sentences were pronounced (of which 2 related to ML).

5.2.2.12. Insider trading and market manipulation

The level of threat from insider trading and market manipulation is assessed low due to the low volume and low complexity of domestic trading, the type of financial instruments admitted to trading (mostly debt instruments), the likely low proceeds and the enhanced transparency of the activity in

[265] Organized Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

[266] See for instance, Organized Crime Portfolio, *From Illegal Markets to Legitimate Businesses: The Portfolio of Organized Crime in Europe*, 2015 (link)

[267] Transcrime, *Study on Extortion Racketeering: The Need for an Instrument to Combat Activities of Organised Crime*, 2009 (link)

[268] Luxembourg Times, 2018 (link)

[269] Regarding the potential amount involved, it is uncertain if the amount discovered during investigation stems from just the extortion offence, other criminal or legal activities

[270] CRF data; per the exchange rate on 30.12.2019

Luxembourg (members and participants of the Luxembourg Stock Exchange are exclusively regulated firms).

The Luxembourg Stock Exchange is large in size in terms of the value of listings, with 3 000 listed issuers coming from over 100 countries[271]. The total amount of debt issued via instruments admitted to trading on the Luxembourg Stock Exchange in 2019 was €1 210 billion[272], representing 1 905% of the GDP of 2019. The Luxembourg Stock Exchange is mainly a debt issuance market, which is reflected in the type of trading conducted (mainly debt securities) and the low value of actual transactions turnover contributes to low risk. The trading volume in 2019 on both trading venues operated by the Luxembourg Stock Exchange was €96.8 million in 2019, representing 0.15% of GDP. The value of equity trading was €45.7 million in 2019[273]. Furthermore, the trading volume is relatively low compared to major European centres such as London or Frankfurt, and the securities sector is small compared to other activities in Luxembourg's financial sector itself.

There have been very few isolated cases of insider trading and market manipulation in Luxembourg in the past three years. More precisely, from 2017 to 2019, the CSSF has conducted 13 investigations on market abuse, and pronounced administrative sanctions in three cases. The most relevant case of market abuse resulted in an administrative fine imposed by the CSSF in 2017 of €1 million; however, this sanction is currently being appealed.

Furthermore, from 2017 to 2019, the CSSF has received and examined 114 suspicious orders and transaction reports from Luxembourg credit institutions, investment firms and trading platforms (the vast majority of which concerned financial instruments admitted to trading on foreign trading venues and were transmitted to the relevant foreign competent authorities) and 76 such reports transmitted to the CSSF from other European competent authorities.

Finally, it should be noted that from 2017 to 2019 the CSSF has assisted other competent authorities in 109 requests for cooperation in potential market abuse cases. This illustrates that the majority of the suspicious transactions on financial markets take place on the more liquid trading platforms operated outside of Luxembourg.

In 2017-2019, the prosecution authorities opened 5 new cases for investigation, implicating 11 persons (none of the cases were related to potential ML) and no prosecution was initiated during the period (with no asset seizures associated)[274]. Moreover, the CRF only reported 12 STR in 2019. The CRF transmitted no files on insider trading and market manipulation to the prosecution authorities in 2019.

Importantly, insider trading and market manipulation (both as a result of the high volatility of financial markets increasing the risk of persons trying to take advantage of inside information, as well as persons in possession of inside information using insecure communication channels due to remote working arrangements) have been highlighted as increasing threats in the context of COVID-19. Further detail is provided in section 4 of the NRA on the impact of the COVID-19 pandemic.

5.2.2.13. Other crimes

The remaining predicate offences have been assessed to represent a lower threat for ML of proceeds of domestic crimes in Luxembourg:

- **Smuggling:** There is limited smuggling of goods into Luxembourg due to low domestic prices (for instance on cigarettes, fuel and alcohol). Taking legally purchased goods out of the country is not

[271] PWC, The *Luxembourg Stock Exchange, A Prime Location for listing*, 2014 (link)

[272] FESE data

[273] FESE data

[274] Data received from Parquet Général Statistical Service in August/September 2020

a predicate offence in Luxembourg. There have been a low[275] number of cases of undeclared cash at borders.

- **Illicit trafficking in stolen and other goods:** There are few reported cases in Luxembourg of trafficking in stolen or other goods (e.g. precious metals, gems, cultural goods and radioactive material). The freeport may increase the threat, but controls are in place. (Note: "common" goods stolen are captured under "Robberies and theft" above).
- **Environmental crimes:** Proceeds of crimes (e.g. related to waste management services, emission schemes, environment standards or wildlife) are deemed low due to the small geographical size and population. Nonetheless environmental/wildlife harm can have long-lasting effects.
- **Illicit arms trafficking:** There are few reported cases in Luxembourg, even though the logistics infrastructure may increase the threat (i.e. storage and transportation).
- **Counterfeiting currency:** There are no recorded incidents of individuals/organized crime in Luxembourg counterfeiting currency on a large scale. Recorded cases by the police concern confiscation and interception of counterfeited currency particularly at banks (upon closing numbers of cash retrieved from circulation), as well as some individuals printing counterfeited currency (typically in low quality and low amounts). In 2017, 63 cases were reported by the police.
- **Murder, grievous bodily injury:** Luxembourg has a very low murder rate and within those, the vast majority of cases are opportunistic rather than by hired assassins or organized crime ("passion crimes"). Hence there are very little proceeds possible to be laundered.
- **Kidnapping illegal restraint, and hostage taking:** There are very few reported cases, and crimes are carried out by individuals rather than by organized crime. Hence, there are very little proceeds possible to be laundered.
- **Piracy:** While there were legal cases opened for piracy (mostly due to merchant vessels flying the Luxembourg flag) the Grand-Duchy has no open sea access and no known river piracy making this predicate offence very unlikely for ML.

5.3. Terrorism and terrorist financing

Terrorism is a global threat with high social and economic costs. In 2018, 71 countries had at least one fatality from terrorism, and 103 countries had at least one terrorism incident. Its estimated global costs were $33 billion, without accounting for indirect impacts on investment, business activity and costs associated with measures countering the financing of terrorism (CFT). Terrorist activity continues to dynamically adapt to changing environments. For example, the activity of jihadist networks in the EU Member States has shifted from recruiting foreign terrorist fighters into the Middle East to conducting their operations in the EU. Terrorist groups increasingly use the internet to promote goals, but also for operational activities, such as recruiting, fundraising, or collecting bomb-making knowledge from online sources.

Together with the terrorism threat, the means used for terrorist financing (TF) continue to evolve. While terrorist financiers continue to use cash, gold and bank wire transfers to raise or move funds, they also increasingly use new and alternative methods. Terrorists have been observed to use virtual assets, prepaid cards and online crowdfunding websites, which now represent an emerging

[275] Note there is only an obligation to declare cash at borders for non-EU cross-border cash movements, but not within EU. Within EU, the obligation is only to disclose upon request. Penal reports are filed by the Customs Authority upon carrying out controls and if an offence is discovered, such as finding undeclared cash where declaration is mandatory, false declarations, and/or refusals to declare upon request by the Authority. See section on Administration des Douanes et des Accises (ADA) and CRF for details.

vulnerability. The combination of the usage of both traditional and financial methods increase the challenges for public authorities and private entities in conducting CFT controls, especially for major international financial centres.

Even though Luxembourg has no detected terrorist activity and had no terrorist attacks in the recent past as of August 2020, the TF risk is significant. In all three countries that Luxembourg borders (Germany, France, Belgium), there have been terrorist attacks with civilian victims in the past five years. Furthermore, Luxembourg is a major financial centre, with a significant presence of traditional financial institutions, such as banks or investment funds, and technologies companies that offer new and alternative payment methods. Those factors make Luxembourgish entities vulnerable to TF misuse and abuse to finance terrorist activity in other countries.

The risks related to terrorist financing will be further analysed in a specific vertical risk assessment to be delivered by the end of the year.

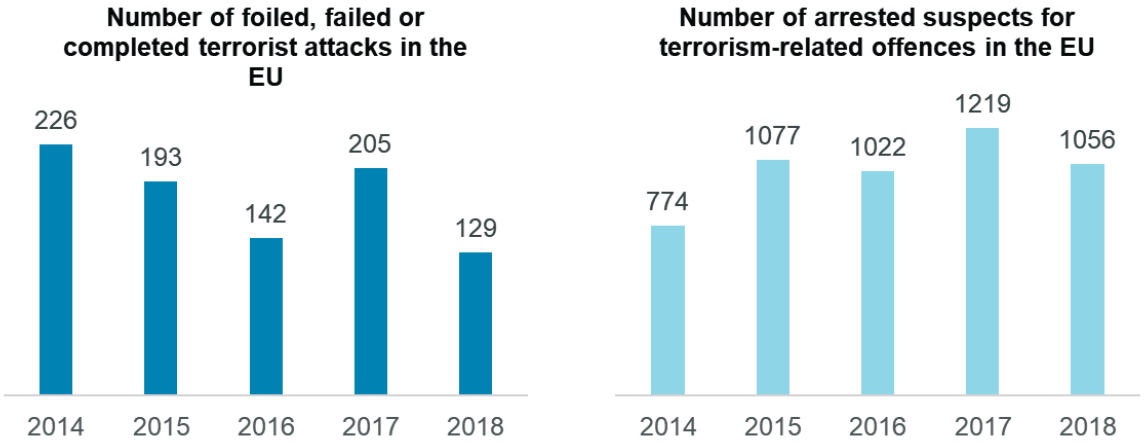
5.3.1. Terrorism threats

Despite no terrorism events in the past and no known terrorist groups in Luxembourg, terrorism is currently a real threat across Europe, and countries near or neighbouring Luxembourg have been affected significantly in recent years. For example, the November 2015 Paris attacks killed 138 people, the Nice truck attacks in 2016 killed 87 people, the 2016 Brussels bombings killed 35 people, and the February 2020 Hanau in Germany shootings killed 11 people.

The total number of terrorist attacks in the EU (failed, foiled or completed) has been larger than this, with 129 in 2018, 205 in 2017 and 142 in 2016[276] (as shown in Figure 12 below). The total number of arrests in the EU for terrorism-related offences has been relatively stable in the past years, totalling about 1 056 in 2018[277]. Similarly, none of the 653 convictions in the EU in 2018 for terrorism-related offences were made in Luxembourg. Overall, attacks carried out by ethno-nationalist or separatist groups accounted for the largest proportion of attacks. Nearly all reported casualties and fatalities in 2018 were the result of jihadist terrorist attacks[278]. In 2018, terrorist attacks caused 13 fatalities in the EU, a large decrease compared to 62 fatalities in 2017. In the past years, terrorist attacks primarily targeted civilians and private enterprises, followed by public institutions and representatives of law enforcement (police and military forces).

[276] Europol, *European Union Terrorism Situation and Trend Report*, 2018 and 2019
[277] Europol, *European Union Terrorism Situation and Trend Report*, 2019
[278] Europol, *European Union Terrorism Situation and Trend Report*, 2019

Figure 12: Number of terrorist attacks and terrorism-related arrests in the EU, 2014-2018[279]

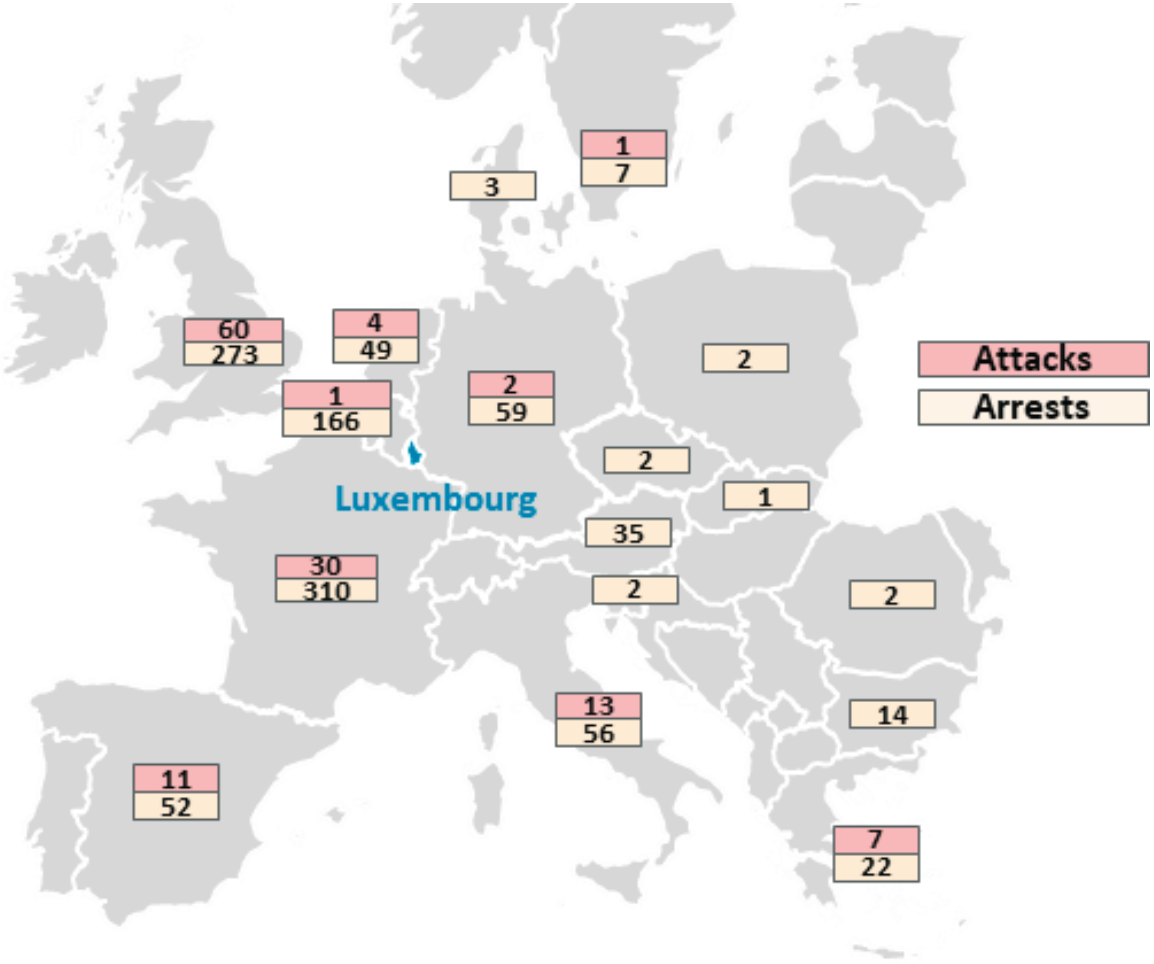


A relatively large proportion of terrorism-related offences and arrests in the EU in 2018 have been made in Luxembourg's neighbouring countries (in particular France with 30 attacks and 310 arrests in 2018), as shown in Figure 13 below. In 2018, most arrests were performed in suspicion of participating in activities of a terrorist group; planning; and preparing attacks. Most arrests in 2018 were related to jihadist terrorism (511 out of 1 056). The number of arrests related to left-wing and right-wing terrorism remained comparatively low, with 44 and 34 arrests respectively in 2018[280].

[279] Europol, *European Union Terrorism Situation and Trend Report*, 2018 and 2019

[280] Europol, *European Union Terrorism Situation and Trend Report*, 2019

Figure 13: Terrorist attacks and arrests by EU Member State in 2018[281]



Following the Paris attacks in 2015, Luxembourg has increased its terrorist threat level to 2 (on a scale of 4), which it has maintained through 2019. This defines a real yet abstract threat; it consists of "increasing vigilance against an imprecise threat and to implement measures of vigilance, prevention and protection of variable and temporary intensity". The government plan "VIGILNAT" defines Luxembourg's national framework for the vigilance, prevention and protection with respect to potential or committed terrorist attacks on national territory as well as governmental actions to be taken[282].

However, several factors increase the overall threat level:

- Luxembourg's geographical proximity to countries having experienced terrorist events and with known presence of terrorist cells (e.g. France and Belgium as referred to above) may contribute to the terrorism threat. This proximity, coupled with open borders within the EU common market and Luxembourg's central geographical position in Europe may give potential terrorists the illusion of escape by car of public transport.
- Jihadist terrorist attacks in Europe have, amongst others, targeted symbols of authority (Paris: February, June and August 2017) and symbols of Western lifestyle (Manchester: May 2017)[283]. As

[281] Europol, *European Union Terrorism Situation and Trend Report*, 2019
[282] Grand-Duchy of Luxembourg website, *InfoCrise: VIGILNAT, Plan Gouvernemental* (link)
[283] Europol, *European Union Terrorism Situation and Trend Report*, 2018

such, the high number of international or multilateral institutions in the Grand-Duchy, or high-profile public events (e.g. music concerts) could expose Luxembourg to terrorist attacks if perceived as attractive targets.

- Jihadist attacks are committed primarily by home-grown terrorists, radicalised in their country of residence without having travelled to join a terrorist group abroad. This group of home grown actors is highly diverse, consisting of individuals who have been born in the EU or have lived in the EU for most of their lives, may have been known to the police but not for terrorist activities and often do not have direct links to the Islamic State or any other jihadist organisation[284].

Terrorism remains a threat to EU countries and Luxembourg. Each year, there are more than 100 foiled, failed or completed terrorist attacks in the EU, and more than 1 000 suspects are arrested for terrorism-related offences. There have been terrorist attacks with killed victims in all three countries that Luxembourg borders in the last five years. While there are no known terrorist groups operating in Luxembourg as of August 2020, multiple factors increase the terrorism threat to Luxembourg, including the presence of international institutions and a significant migrant community. Overall, the terrorist threat in Luxembourg is assessed as real, but abstract.

5.3.2. Terrorist financing threats

In general, there are three stages to terrorist financing: the raising of funds, through either illicit or licit activities; the moving of funds; and the using of funds. Terrorist financing not only involves the direct financing of acts of terrorism, but also the financing of propaganda, recruitment, training, travel, daily living expenses and other operational needs of an individual terrorist or terrorist group.

5.3.2.1. Foreign terrorist fighters (FTFs)

Globally, the two most common methods for FTFs to raise funds are self-funding and funding by recruitment and facilitation networks[285]. For self-funding, the most common funding sources include salaries, social benefits, non-paid-off consumer loans, overdraft from bank accounts and donations from family and friends. Recruitment and facilitation networks will typically have specific recruiters that support FTFs financially and materially, including arranging transportation and purchasing supplies[286].

Luxembourg is one of the countries in the EU least affected by FTFs travelling to conflict zones (mostly Syria and Iraq)[287]. However, there are a few known cases of Luxembourg nationals having joined the Islamic State.

It is important to note that the funding needs of FTFs are typically very low and pose significant detection challenges, globally and for Luxembourg. For example, the level of funding of an FTF usually falls below €10 000[288], which is below the minimum amount of 2010 Cash Control Law. Similarly, transactions made by FTFs using banks or MVTS providers would not always trigger additional checks due to low amounts involved.

5.3.2.2. Lone actors and small terrorist cells

Similar to FTFs, lone actors and small terrorist cells recently been mostly funded through small amounts and involved funds usually sourced from legitimate activities such as retail businesses, amongst others. In addition to licit employment incomes, state subsidies and social benefits, funds

[284] Europol, *European Union Terrorism Situation and Trend Report*, 2018

[285] FATF, Emerging terrorist financing risks, 2015

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

[287] European Parliament press briefing: Combating terrorism, September 2017 (link)

[288] Oftedal for the Norwegian Deference Research Establishment, *The financing of jihadi terrorist cells in* Europe, 2015

provided from like-minded individuals within the community can also be sources of income for lone actors.

Luxembourg shares the factors that drive the TF threat of lone actors and small terrorist cells globally. The channels used to move raised funds could be legitimate, regulated channels (e.g. bank wire transfers) but also illegal, difficult to detect channels such as hawala. Additionally, identifying financial transactions used for terrorist financing is extremely difficult as these could very easily be confused with legitimate activities (e.g. withdrawal from current accounts). Similar to FTFs, lone actors and small terrorist cells can receive funding or recruit from radicalised youth.

5.3.2.3. International terrorist organisations

Globally, international terrorist organisations may use a variety of methods to raise funds. They may raise funds through private donations, and wealthy private donors may in particular form an important source of their income[289]. They may also use proceeds of criminal activity, such as drug trafficking, fraud and smuggling of goods. As many 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. A growing source of income for terrorist organisations is kidnapping for ransom: between 2008 and 2014, terrorist organisations, including al-Qaida and ISIL, reportedly generated at least $222 million in ransom payments[290].

In Luxembourg, there are no known international terrorist organisations present as of August 2020. However, there is still a threat of terrorist financing. The Luxembourg finance industry may be misused to send funds to international terrorist organisations in other countries. NPOs based in Luxembourg may also execute projects in territories, which are in close proximity to terrorist organisations. The materials and funds of those projects may be misused for terrorist financing.

5.3.2.4. Other terrorist actors

State sponsors of terrorism and terrorist safe havens can enable terrorists to raise or move funds. For example, Iran's support to Hezbollah has been estimated to reach up to $700 million per year, accounting for the majority of Hezbollah's annual budget[291]. State sponsors of terrorism and terrorist safe havens can also promote illicit activities that generate funds for terrorists or allow their financial systems to be misused for funds movement. For example, the Assad regime in Syria allowed banks in territories controlled by ISIL to continue operating[292].

Luxembourg faces the threat that entities operating from it may be misused for sending funds or other forms of support (e.g. philanthropy) to state sponsors of terrorism, which may be then used to finance terrorism. Furthermore, support sent by Luxembourg NPOs may be abused by terrorist organisations operating in safe havens, particularly when local governments in safe havens have poor governance controls.

'Corporate' terrorist groups by definition have advanced and significant financing capabilities. For example, FARC had an annual income from illegal drug production estimated to be between $0.2 to $3.5 billion, according to various reports[293,294]. Other methods that 'corporate' terrorist groups could

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

[290] FATF, *Emerging terrorist financing risks*, 2015

[291] US State Department, *Country Reports on Terrorism*, 2019

[292] Committee on Political Affairs and Democracy, *Funding of the terrorist group Daesh: lessons learned*, 2018

[293] Insight Crime, *The FARC, the peace process and the potential criminalization of the guerillas*, 2013

[294] John Otis - Wilson Center Latin American Program, *The FARC and Colombia's Illegal Drug Trade*, 2014

use for financing include fraud, kidnapping for ransom (e.g. pirates cooperating with jihadist groups), robbery and theft.

In Luxembourg, there are no known 'corporate' terrorist groups operating. However, similar to the state sponsors of terrorism and terrorist safe havens, Luxembourgish entities could be misused or abused for financing terrorism activities by those terrorist groups.

6. INHERENT RISK – VULNERABILITIES

This section presents findings of the inherent vulnerabilities (sectors) assessment performed as described in the methodology section.

Vulnerabilities are "those things that can be exploited by the threat or that may support or facilitate its activities"[295]. In the context of this NRA, vulnerabilities in Luxembourg arise from sectors, which are particularly exposed to misuse or abuse for laundering and terrorist financing purposes.

Note that inherent vulnerability is defined as the vulnerability of a sector to be abused or misused for ML/TF *before* mitigating actions are considered. As described in the methodology section, the National Risk Assessment focuses on the macro- and meso-level analyses. Results of this National Risk assessment and of meso- and micro-level assessment done by agencies were aligned were relevant and any differences in results were reviewed and discussed to understand the reasons for the discrepancy.

6.1. Summary of findings

Luxembourg's inherent vulnerabilities are high across most sectors, but lower in market operators, support PFSs and other specialised PFSs, insurance, gambling and dealers in high-value objects. Table 13 (below) provides an overview of the inherent vulnerabilities at a sector level.

Table 13: Inherent vulnerabilities - by sector[296]

Sector		Inherent risk
1	Banks	High
2	Investment sector	High
3	MVTS	High
4	Specialised PFSs providing corporate services	High
5	Market operators	Low
6	Support PFSs & other specialised PFSs	Very low
7	Insurance	Medium
8	Professional service providers	High
9	Gambling	Low
10	Real estate	High
11	Dealers in goods	Medium
12	Freeport operators	High
13	Legal entities and arrangements	High

Table 14 (below) shows the assessment of the level of vulnerability of the financial and non-financial sectors at a more granular level (such as the sub-sector level).

[295] *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment,* February 2013

[296] At the time of writing the NRA (July 2020), the Ministry of Justice is in the process of conducting a vertical risk assessment on VASPs. These entities became obliged entities only in 2020, with CSSF designated as competent authority for their AML/CFT supervision, and therefore they are not included in the table

Table 14: Inherent vulnerabilities - by sub-sector[297]

Sector		Inherent risk	Sub-sectors	Inherent risk (sub-sector)
1	Banks	High	Retail & business banks	4.0
			Wholesale, corporate & investment banks	3.9
			Private banking	4.4
			Custodians and sub-custodians (incl. CSDs)	3.7
2	Investment sector	High	Wealth and asset managers	3.6
			Brokers and broker-dealers (non-banks)	3.6
			Traders / market-makers	2.7
			Collective investments	4.1
			Regulated securitisation vehicles	2.9
			CSSF-supervised pension funds	2.0
3	MVTS	High	Payment institutions	3.6
			E-money institutions	3.6
			Agents and e-money distributors acting on behalf of PI/EMIs established in other European Member States	3.0
4	Specialised PFSs	High	Specialised PFSs providing corporate services	3.9
			Professional depositaries	2.8
5	Market operators	Low	Market operators	2.3
6	Support PFSs & other specialised PFSs[298]	Very low	PFSs de support	*N/A*
			Other specialised PFSs	
7	Insurance	Medium	Life insurers	4.1
			Non-life insurers	2.6
			Reinsurance	2.6
			Intermediaries	3.4
			Professionals of the insurance sector (PSA)	1.9
			CAA-supervised pension funds	1.8
8	Professional service providers	High	Lawyers	3.9
			Notaries	3.7
			Bailiffs *("Huissiers de justice")*	2.8
			(Approved) statutory auditors and (approved) audit firms *("Réviseurs d'entreprises (agréés)" and "cabinets de revision (agréés))*	3.8
			Chartered professional accountants *("Experts-comptables")*	4.0

[297] At the time of writing the NRA, the Ministry of Justice is in the process of conducting a vertical risk assessment on VASPs. These entities became obliged entities only in 2020, with CSSF designated as competent authority for their AML/CFT supervision, and therefore they are not included in the table

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

Sector		Inherent risk	Sub-sectors	Inherent risk (sub-sector)
			Accountants and tax advisors	4.1
			TCSPs – Administrateurs / directors[299]	4.1
			TCSPs – Business offices[300]	4.1
9	Gambling	Low	Casino	2.8
			Sports betting[301]	*N/A*
			Ad hoc lotteries	2.0
			National lottery	1.9
			Online gambling[302]	*N/A*
10	Real estate activities	High	Real estate agents *("agents immobiliers")*	4.1
			Real estate developers *("promoteurs immobiliers")*	4.1
11	Dealers in goods	Medium	Precious metals/jewellers/clocks	3.0
			Car dealers	3.9
			Art/Antiques	2.7
			Luxury goods *(e.g. "maroquinerie")*	3.1
12	Freeport operators	High	Freeport operators	3.7
13	Legal entities and arrangements	High	*Sociétés commerciales*	4.4
			Domestic "fiducies"	4.8
			Foreign trusts	4.8
			Associations sans but lucratif (ASBL) and *fondations* with Non-governmental organisations (NGO) status	3.6
			Sociétés civiles	3.2
			Other *associations sans but lucratif (ASBL)*	2.2
			Other *fondations*	1.8
			Other legal entities	2.0

6.2. Detailed assessment by sector

As explained in the methodology section, the sectors in-scope for this assessment were arrived upon by how the supervision of these sectors is organised under the various public-sector supervisory authorities. Therefore, this assessment involves sectors not mapped based on activity but based on supervisory setup.

The inherent vulnerabilities rating does not take into account the vulnerability level once controls are in place, which is covered under the residual risk sections.

[299] Analysis covered in NRA vulnerability section; TCSPs under AED supervision are assessed on aggregate
[300] Analysis covered in NRA vulnerability section; TCSPs under AED supervision are assessed on aggregate
[301] Analysis covered in NRA text version. No separate scorecard in appendix as activity not present in Luxembourg
[302] Analysis covered in NRA text version. No separate scorecard in appendix as activity not present in Luxembourg

6.2.1. CSSF supervised sectors

6.2.1.1. Banks

The **banking** sector is naturally vulnerable to ML/TF risks due to a variety of drivers such as the large customer base, high transaction speed and the large volume of financial flows, which, pursuant to the general understanding of ML practices worldwide, could potentially facilitate the concealment of illegal transactions. Also, criminals laundering money or financing terrorism might attempt to conceal the origin of their money and integrate it into the formal economy by using the financial system.

Historically, this sector has offered strong professional secrecy, but this factor has been heavily limited in impact through regulatory changes[303]. Those include the introduction of the (worldwide) exchange of information with all tax authorities adhering to the OECD's common reporting standard and the law of 23 December 2016 subjecting aggravated and organised tax fraud to penal sanctions so that it forthwith constitutes a primary offence of money laundering (hereafter the 2017 Tax Reform Law). In addition, the transposition of the EU Directive 2011/16 on Administrative Cooperation in Direct Taxation and its amendments and the Law of 13 January 2019 introducing the beneficial owner register further reduced the historical professional secrecy of the sector. More recently, the 2020 RBASD Law obliged Luxembourg (credit) institutions to set up systems containing information on payment accounts and safe-deposit boxes holders that allow access to this data by the CSSF, the CRF and other competent stakeholders.

This sector includes all the activities carried out by entities with a banking license (chapter 1 of 1993 LSF Law) and includes retail and business banking (including payment services), wholesale, corporate and investment banks, private banking and custodians and sub-custodians (including CSDs).

The banking sector in Luxembourg is potentially exposed to ML/TF risks. Firstly, the **size of the banking sector is large** when compared to the size of the overall economy in Luxembourg. The 128 banks from 27 different countries[304] represent ~20% of contribution to the GDP[305], with €823 billion[306] in assets representing ~12 times GDP as of the fourth quarter 2019, and more than 26 000 people employed[307]. The banking sector in Luxembourg overall had €26.6 billion revenues in 2018.

Secondly, banks in Luxembourg have considerable exposure to **international business** as only eight banks are domestic, and the 120 other banks originate from foreign countries. For example, in private banking, less than a quarter of private banking AuM comes from Luxembourg, while the rest of the assets come from abroad[308]. The international client base is driven by Luxembourg's political and the juridical stability, the high and non-discriminatory property protection rules, the stable and well-regulated banking sector, its well-established reputation among professionals and investors, the quality of its service providers and the broad range of financial services offered in Luxembourg, in particular the investment sector and its products.

Thirdly, the **large number of customers** together with a **proportion of high-risk customers** may increase ML/TF risks. In 2019, there are approximately 5 million accounts opened in Luxembourg banks. In addition, two e-commerce institutions with a banking license operating e-payments have

[303] Further details can also be found in the Detection and Prosecution of the NRA, which highlight that there is no banking secrecy with regards to the CRF (as per article 5(1) of the 2004 AML/CFT Law) and which highlight that professional secrecy obligations do not apply to orders from magistrates.

[304] Banque Centrale du Luxembourg, *Statistiques : Etablissements de crédit ; „tableau 11.01" and „tableau 11.05"* as of February 2020 (link)

[305] STATEC

[306] CSSF *data*, 2019

[307] Banque Centrale du Luxembourg, *Statistiques : Etablissements de crédit ; „tableau 11.02"* as December 2019 (link)

[308] CSSF, ML/TF sub-sector risk assessment Private Banking, 2019

approximately 95 million accounts. Of all accounts opened at institutions with a banking licenses, ~0.1% are classified as high-risk, and ~0.02% are linked to PEPs[309].

The banking sector is globally viewed as significantly vulnerable to ML/TF risks[310]. Similarly, it is deemed as high risk in Luxembourg. The assessment is sub-divided into sub-sectors along with retail and business banks, wholesale and investment banks, private banks and custodians, as summarised in the table and sub-sections below.

As the contraction in Luxembourg's economic activity could place some entities in distress (e.g. commercial borrowers such as corporates and SMEs), which in turn has the possibility to create opportunities for them to be exploited by criminals seeking to launder illicit proceeds. Further detail is provided in section 4 of the NRA on the impacts of COVID-19.

Retail and business banks

Worldwide**, retail and business banks** have been abused for ML/TF as they may offer services to cash-intensive businesses, have a high volume of transactions and offer a diverse set of products.[311] They may be abused for laundering proceeds from a wide range of predicate offences, which increases the difficulty for detection and prevention due to the high speed of transactions, the ability to withdraw funds in cash or transfer funds to another country. For example, in France, it has been observed that a person laundered money for a drug trafficking organisation by depositing cash into a bank account, and then withdrawing the deposited money from an ATM in a different country in local currency[312]. Retail banking has also been abused for moving terrorist funds or raising funds for terrorist activities. For example, in the UK, there have been cases of terrorists raising funds through credit fraud or loan fraud, in which individuals falsely claimed to have been defrauded, expecting banks to refund them[313]. Further, retail bank customers typically do not act via direct contact but through online banking, which may increase customer anonymity features and thus increase ML/TF risks.

In Luxembourg, retail and business banks are vulnerable to ML/TF because of the nature of products offered, the sector size in Luxembourg and their international clients and transaction flows. The products offered are inherently vulnerable to ML/TF, as they could be misused by criminals to place laundered money in the financial system and but more specifically to layer the funds in the Luxembourg context.

ML/TF risks are driven by the **sub-sector size** of retail and business banking. There are 15 entities[314] with total assets of €167 billion[315] in the sub-sector as of December 2019[316]. They have a large stock of customers with ~1.2 million[317] clients and total income amounting to €8.4 billion[318]. However, note that the ~1.2 million customers are mostly explained, as most Luxembourg residents have several accounts and with several banks and by the large number of cross border commuters[319]. The ML/TF

[309] CSSF *data*, 2019

[310] See for example EBA, *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, 2019

[311] FATF, *Risk-Based Approach for the Banking Sector*, 2014

[312] OECD, *Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*, 2009

[313] HM Treasury, National risk assessment of money laundering and terrorist financing, 2017

[314] CSSF *data*, 2018

[315] CSSF *data,* 2019

[316] CSSF *data*, 2019

[317] ABBL RBS/CSSF *data,* 2018

[318] CSSF *data,* 2019. Total income (gross) as the sum of interest income, dividend income, fees income, other operating income, P&L trading book & P&L banking book

[319] Note that this figure excludes the number of clients of two e-commerce institutions providing services under a banking licence

risk is **partially reduced by the high concentration** of the sub-sector, with the top five entities representing 89% of the market assets[320].

Note that the **exposure to geographies with weak AML/CFT measures is limited** (0.1% of assets and 0.2% of liabilities)[321]. Thus, the ML/TF risk is reduced here.

As described above, part of the ML/TF risk is also increased by the nature of products. The **payment services activity** carried out by retail and business banks is potentially vulnerable to ML risks, also in Luxembourg, as they can experience layering and extraction techniques used by criminals which are comparatively more sophisticated than in other sub-sectors. For instance, common methods used are funding of a product using one method and withdrawal using another. For example, terrorist actors could misuse/abuse retail banking products to move funds cross-border by opening a current account and using the associated debit card to withdraw funds overseas (e.g. in a conflict zone or where an attacked is planned).

Wholesale, corporate and investment banks

Wholesale, corporate and investment banks are seen to be very high risk globally. Some products (especially those with international flows) are more exposed to ML/TF, such as trade finance and correspondent banking. Since trade finance involves several cross-border transactions, multiple participants and large sums, it is deemed to be particularly risky. As for Luxembourg's limited correspondent banking activity, the risk is mostly driven by cross-border correspondent banking relationships when banks execute third-party payments and thus may have limited visibility on them[322].

The sub-sector's vulnerabilities are compounded by the **large volume of transactions**, which are quick, efficient and international. r

The **international nature of business** also increases the risk as 77% of assets are outside of Luxembourg. Flows with geographies with weak AML/CFT measures are limited (0.3% of assets and 0.2% of liabilities; for intragroup treasury, respectively 0.2% and 0.0%)[323].

Note that the sub-sector is **relatively concentrated** (the top five entities represent 60% of the market[324]), which makes it easier to monitor and detect potential ML/TF activities. Finally, the risk is reduced by the **low-risk nature of clients**, which are a smaller number of mostly institutional customers (financial institutions contribute to more than 80% of the deposits[325]).

Custodians and sub-custodians (incl. CSDs)

Custodians could be vulnerable to ML/TF risk since they deal with a large number of transactions across multiple customers when providing securities-related services to clients. The risk may be increased in the cases of omnibus accounts, in which assets are held in the name of the intermediary and not in the name of the ultimate beneficial owner. Globally, there have been cases where intermediaries were used to avoid economic and financial sanctions through omnibus accounts[326].

In Luxembourg, the ML/TF risk is primarily driven by the **high share of international business**. Custodians are likely to have international clients (72% of assets and 54% of liabilities are outside

[320] CSSF *data,* 2018

[321] BCL *data* (countries in scope are those that FATF defines as "high risk and other monitored jurisdictions")

[322] FATF, *Guidance on correspondent banking services*, 2016

[323] CSSF *data,* 2018

[324] CSSF *data,* 2018

[325] CSSF *data,* 2018

[326] ISSA, *Study on the Benefits and Costs of Securities Accounting Systems*, 2015

Luxembourg[327]). However, flows with **geographies with weak AML/CFT measures are limited** (0.05% of assets and 0.35% of liabilities[328]).

The risk is also driven by the **size of the sub-sector**. In Luxembourg, the sub-sector consists of 29 entities[329] resulting in a total income of €5.73 billion[330] and assets of €179.4 billion[331]. Concurrently, the market in Luxembourg **is relatively concentrated** with the top five entities accounting for almost two-thirds of the assets which facilitates monitoring and helps limit risk.

Further, since custodians mostly deal in fairly **commoditised and standardised products** (e.g. custody of shares, dividend and interest payment collection and distribution), their risk is restricted with regards to ML and TF. As such, their overall ML/TF vulnerability is lower than for other banking sub-sectors.

CSDs' ML/TF vulnerability results from the large volume of frequent and high-value transactions, which adds to detection challenges. Furthermore, CSDs are exposed to cross-border flows. However, in Luxembourg, the risk is mitigated due to the **very high sector concentration**. Out of the two players, only one player has a banking license with revenues of €974 million. In addition, customers are limited to a group of selected institutional members, limiting the **client risk**.

Private Banking

Private banking is known to be subject to ML/ TF risks. The key risk drivers for private banking stem from the significant exposure to international clients, high concentration of high net worth clients, and the complexity of some products (e.g. wealth structuring activities). The 2019 Private Banking SSRA identified that for Luxembourg, there are three predicate offences especially relevant to the sub-sector: tax crimes, corruption and bribery, and fraud. Although private banking may be abused for terrorist financing, especially through products that allow cross-border payments, the overall TF risk for private banking is smaller than for retail banking. Case Studies 4 and 9 (in the "threats assessment" section) and Case Study 10 (below) provide examples and typologies[332] to highlight how private banking can be abused for ML/TF purposes:

Case Study 10: Private banking and terrorist financing (non-Luxembourg case) [333]

An EU foundation used its private bank account to deposit large amounts of cash and transfer them to companies with strong links with EU-listed terrorist organizations. The private banking client, head of a Non-Profit Organization, deposited large amounts of cash on the foundation's account. Funds were transferred via an international bank payment to an IT support provider and a publishing company in another EU member state. Investigations showed there was a strong link between the head of the Non-profit organization and an EU-listed terrorist organization.

[327] CSSF *data,* 2018
[328] CSSF *data,* 2018
[329] CSSF *data,* 2018
[330] CSSF *data,* 2018
[331] CSSF *data,* 2018
[332] Case studies and typology used from the CSSF, *Sub-sectoral Risk Assessment Private Banking*, 2019
[333] FATF, Financing of Recruitment for Terrorist Purposes, January 2018

In Luxembourg[334], the private banking sub-sector is well developed with 39 entities offering mainly private banking activities serving ~172 000 customers generating about €5.8 billion of net income and accounting for €395 billion assets under management as of 2018[335].

The **size and fragmentation** of the private banking sector increase the ML/TF vulnerability of the sub-sector. Most private banks in Luxembourg are part of international groups. There are several large banks, but also many smaller institutions competing for a share of the market. Smaller banks may also specialise in specific types of clients (e.g. affluent vs. UHNW clients only, or clients from specific geographies or affiliated with a specific group). This focus, together with their limited size and typically limited resources, may increase the risk level of smaller private banks.

The risk is further driven by the **nature of clients**. The prevalence of big and potentially more sophisticated accounts may increase the complexity of private banking activities performed in Luxembourg. Clients with AuM larger than €1 million hold a large and increasing majority of private banking AuM in Luxembourg. According to private banks' own internal risk assessments, a large percentage of their clients have high ML/TF risk. The percentage of high-risk clients in Luxembourg private banks is much higher than in other banking sub-sectors such as retail banks.

This sub-sector is very exposed to **international flows** both in terms of assets and entities' origin, which increases the vulnerability to foreigners misusing the sub-sector's entities for ML/TF purposes. In terms of geographical origin, according to the CSSF-ABBL survey and CSSF internal data, the majority of AuM comes from Europe, but outside Luxembourg. This may complicate the identification of beneficial owners and the origin of their wealth. Less than a quarter of private banking AuM comes from Luxembourg account-holders, while the remaining three quarters come from account-holders located abroad[336,337]. While the diverse, international clientele reflects the attractiveness of Luxembourg as an international private banking centre, the cross-border origin of most AuM may decrease the level of transparency on the funds invested in the sub-sector.

A number of banks use **intermediaries** in providing private banking activities. Intermediaries used by private banks and their clients can be classified into three main types: introducing intermediaries (sometimes also referred to as "finders"), POA-holders and third-party managers. Whilst the number of accounts and volume of transactions that involve these categories of intermediaries is not especially high, their involvement can increase the distance between the bank and its client. This may reduce transparency on beneficial ownership or source of wealth and therefore increases exposure to threats such as tax crimes, corruption or fraud.

6.2.1.2. Investment sector

Globally, the investment sector is considered to be vulnerable to ML/TF activity as large amounts of money are invested often on behalf of wealthy individuals or entities.

The sector is large and diverse with a variety of entities such as wealth and asset managers, broker-dealers, traders/market makers, UCITS management companies, AIFMs, self- or internally-managed UCIs, pension funds and regulated securitisation vehicles. The detection challenges are not to be underestimated due to high market fragmentation in terms of the number of providers and also the high volume of retail and institutional investors. However, pension funds, regulated securitisation

[334] Text here and below from the CSSF, *Sub-sectoral Risk Assessment Private Banking*, 2019

[335] CSSF *data*, 2018

[336] ABBL/CSSF, *Annual Private banking surveys*, 2013-2018

[337] Note that as the geographic origin of assets is assessed through the origin of client accounts, it is likely the foreign-based beneficial owners represent an even larger share than 76% of AuM.

vehicles and traders/market-makers face low or medium risks due to the nature of their activities or smaller market sizes.

Due to the economic impact of COVID-19, many stock markets and investment products around the world have experienced significant volatility. Where assets are valued at a significant discount, investors may be looking to offload and minimise losses. This could provide an opportunity for criminals offering to purchase or refinance such distressed assets (using the backing of illicit funds). In addition, the contraction in Luxembourg's economic activity as a result of the global pandemic could place some entities in distress, which in turn creates opportunities for them to be exploited for money laundering purposes. Further detail is provided in section 4 of the NRA on the impacts of COVID-19.

Investment firms

Investment firms constitute a smaller part of Luxembourg's financial services sector than banking or collective investments sub-sectors. They encompass several different types of professionals, which can be grouped into three categories: wealth and asset managers, brokers and broker-dealers (non-banks) and traders / market-makers.

As of the end of 2019, there are 97 investment firms established in Luxembourg, with some of investment firms having licenses to exercise multiple activities at once (for example, an investment firm can act as a private portfolio manager, described below, and a broker simultaneously). Investment firms employ 1 690 people and service approximately 100 000 clients at the end of 2019. For wealth and asset managers, and brokers and broker-dealers (non-banks), the ML/TF risk is primarily driven by the **high international business** share and the **nature of clients**. 56 of 97 investment firms have high risk clients, and approximately 4% of total clients are marked as high-risk. The risk is reduced by the fact that 31 entities have **limited AuM from weak AML/CFT** countries, which represent a very small amount of the total AuM.

Wealth and asset managers

The sub-sector **wealth and asset managers** encompasses "private portfolio managers" (article 24-3 of the 1993 LSF Law) and "investment advisers" (article 24 of the 1993 LSF Law).

In Luxembourg, it is a **medium in size and fragmentation** sub-sector. 90 investment firms have the license of investment adviser, with 37 of them exercising those activities. 82 investment firms have the license of private portfolio manager, with 68 of them exercising those activities. Investment advisers have a revenue of €26.5 million (top five firms capturing ~80%) and value of portfolio advised of €6.1 billion (top five firms capturing ~80%). Private portfolio managers have a revenue of €184.2 million (top five firms capturing ~37%) and AuM of €40.6 billion (top five capturing about 45%). Overall, the entities of the sub-sector have approximately 50 000 assigned mandates.

Their ML/TF risk is increased by the substantial **international business** (as described above for investment firms in general) and **foreign ownership** (approximately 37% of them have foreign non-EU ownership, with one entity having an owner from a country with weak AML/CFT flows).

The **products and activities** offered by wealth & asset managers have an impact on the overall ML/TF risk. 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). Note that investment advisers may also carry out some relevant activities, however the materiality of this is considered relatively low. The product risk may also be increased by the presence of omnibus accounts. However, only seven entities have omnibus accounts, accounting for 3.82% of the total AuM.

Brokers and broker-dealers (non-banks)

Brokers include "brokers in financial instruments" (article 24-1 of the 1993 LSF Law), "financial intermediation firms" (article 24-8 of the LSF) and distributors of units/shares in UCIs (article 24-7 of the 1993 LSF Law). **Broker-dealers** (non-banks) include "commission agents" (article 24-2 of the 1993 LSF Law).

Similar to wealth and asset managers, the sub-sector is **medium in size and fragmentation**, with 93 investment firms total with relevant licenses, and only 36 of them exercising them in 2019. Nearly all revenues and transactions (about 98%) are concentrated by the top five entities.

The risk is increased by the **volume of clients and transactions**. In this sub-sector, numerous entities are processing a large number of customers and executing a high volume of transactions. As such, broker-dealers (non-banks) facilitated transactions worth €251.2 billion in 2019, and brokers facilitated transactions worth €122.2 billion respectively, with approximately 75 000 administered mandates. The sub-sectoral risks are also increased due to **significant international involvement**. 32% of brokers and broker-dealers (non-banks) have foreign non-European ownership, whereby only one investment firm is owned by foreign persons/ entities from high-risk countries

The risk is increased by the fact that brokers and broker-dealers offer **non-client- facing businesses** but limited by the fact that the clients are mainly institutional, and the fact that client relationships are initiated face-to-face.

Traders/market-makers

Traders/market-makers include professionals buying or selling securities for the purposes of proprietary trading or market-making activities: Professionals acting for their own account (article 24-4 of the 1993 LSF Law), Market makers (article 24-5 of the 1993 LSF Law) and underwriters of financial instruments (article 24-6 of the 1993 LSF Law). Globally, the ML/TF risk of traders and market-makers have been misused to generate illicit sums of money, through offences such as insider trading, market manipulation and fraud[338].

In Luxembourg, the ML/TF risk stems primarily from the fact that they **manage money for their owners** and that they could be misused for ML/TF purposes. In addition, **international exposure** and **large volumes observed** drive the ML/TF risk.

In Luxembourg, the vulnerability is limited because of the **very small sector size**. As of 2019, there are five investment firms licensed as professionals acting for their own account, with only two carrying out those activities in 2019. There are two investment firms licensed as underwriters of financial instruments, but none of them carry out relevant activities. The total AuM of the investment firms is €44.2 million.

Collective Investments

Globally, collective investments risk to be abused or misused for different types of fraudulent practices, including for example "Ponzi" schemes, confidence or "boiler room" scams, use of fictitious or "shell" companies, misleading investments and misstated value determination. Collective investments can be abused and misused through schemes concerning both liability (inbound investments) and asset (outbound investments) sides. The possible schemes include raising funds from corrupt government-related investors (inbound investments), securing investments in corrupt government-related projects (outbound investments), influencing investment and portfolio allocation

[338] FATF, *Money Laundering and Terrorist Financing in the Securities*, 2009

decisions (outbound investments), and investing in corrupt portfolio companies (outbound investments).

In other countries, there have been some cases of market manipulation via the abuse or misuse of collective investments. For example, the investment fund managers could collude over the price of a security before an IPO. The risk of price collusion is increased in situations with a limited number of investors making high-value investments, in particular in securities which are difficult to price.

Case Study 11: Collective investments and money laundering[339]

In 2018, the administrator of Fund X became aware that one of the fund's investors had requested the full redemption of the units held in the fund. This investor's account had been blocked because the documentation on the origin of the funds was incomplete. As for the investor, it was a tax-opaque Liberian entity.

The funds from the liquidation were to be paid into the investor's Swiss account via a correspondent located in the United States. The investor had never justified the reasons for the complexity of the chosen structure, including shell companies, several changes in the corporate structure, including at the management level, through non-cooperative jurisdictions. It had also not given any explanation on the origin of the funds used to acquire the shares of the fund. Some entities of this structure had been mentioned in the "Panama Papers".

The administrator was unable to remove suspicions of a possible illegal source of funds or even tax evasion.

In Luxembourg, the sector is large and fragmented, and consists of various components with more than €4.73 trillion in AuM across 3 000 plus entities as of December 2019[340]. This sub-section groups collective investments into three main classes: UCITS ManCo (including Super ManCo), AIFM and self or internally managed UCI, each consisting of multiple clustering elements. Each class is mutually exclusive, and all classes taken together cover the full spectrum of regulated collective investments in Luxembourg [341].

UCITS Management Companies "ManCo" (including SuperManCo)

Luxembourg Chapter 15 ManCo include an important number of entities who manage the large majority of assets in Luxembourg in a sector characterised by a relatively high degree of concentration. Luxembourg Chapter 15 ManCo heavily rely on cross-border distribution networks to market their UCI across Europe and in a number of non-EU jurisdictions.

The high inherent risk presented by this category is also explained by the volume of assets under management and the inclusion of entities benefitting from a double license (CH15 and AIFM) in this category. Therefore, the AIFM component of this cluster increases the inherent risk, notably because of the types of investments made by AIFs.

EU/EEA UCITS ManCo act as designated IFM of Luxembourg investment vehicles and are primarily located and supervised in five countries: Germany, France, United Kingdom, Ireland and Italy. Volumes of assets under management are a key risk driver.

339 CRF, *Annual report*, 2018

340 CSSF, *Évolution des actifs nets et du nombre d'OPC*, as of 31st December 2019

341 All information below from the CSSF, *AML/TF sub-sector risk assessment: Collective investments*, released in January 2020

The quality and transparency of distribution channels is also an important risk factor for EU/EEA IFM. Indeed, the relationship between the IFM and end-investors is further distanced due to cross-border management and cross-border distribution, which increases the ML/TF risks.

Alternative investment fund managers ("AIFM")

Luxembourg authorised AIFM are generally of moderate size with most Luxembourg AIFM groups or parent undertakings originating from Switzerland, Germany and Belgium. The sector is characterised by a certain degree of fragmentation, with the top 10 entities representing 31% of total assets and the top 50 entities representing 71% of total assets.

They manage a diverse set of UCI, across different regimes, generally subject to fewer rules and diversification requirements than UCITS. The diversity of such types of investments statistically increases the risk of investing in high ML/TF risk assets.

The geographical reach of Luxembourg authorised AIFM facilitated by EU/EEA passporting agreements increases general ML/TF vulnerability. A portion of the overall distributors marketing funds managed by these AIFMs are not supervised by NCAs or self-regulated bodies for AML/CFT purpose which increases the overall risk of this category.

Luxembourg registered AIFM include a high number of IFM, but their net assets remain low given the AIFMD regulatory threshold capping assets under management at €100 million or €500 million for unleveraged and close-ended AIF. Larger AIF over €100 million managed by registered AIFM must be closed-ended, restricting investor redemption rights during a period of five years. The resulting longer-term nature of the investment limits the risk of ML/TF by developing the business relationship with the investor and delaying the integration of funds back into the economy. However, the types of investments remain less plain vanilla and therefore present higher ML/TF risks.

An important number of Luxembourg Chapter 16 ManCo are active in Luxembourg. Similarly to AIFM, this sector is fragmented. Chapter 16 ManCo not authorised as AIFM do not benefit from a passport to carry out activities outside of Luxembourg. Given this lack of EU/EEA equivalence, Chapter 16 ManCo remain less international than Luxembourg authorised AIFM, reducing ML/TF vulnerability.

Chapter 16 ManCo may manage regulated non-UCITS and non-AIF. These vehicles are subject to less harmonised rules than UCITS and AIF, and have to abide by less requirements. The investment types and areas of Chapter 16 ManCo are relatively diverse, increasing the risk of being exposed to higher ML/TF risk. Chapter 16 ManCo typically invest in less transparent and less liquid assets, potentially increasing ML/TF risks.

A portion of the distributors used for the marketing of their UCIs are not subject to AML/CFT supervision and few UCIs managed are considered by their designated IFMs as having a complex distribution scheme.

EU/EEA AIFMs act as designated AIFM of Luxembourg investment vehicles and are primarily located and supervised in five countries: UK, France, Ireland, the Netherlands and Germany. Most IFM's groups or parents originate from North America (Canada and USA) and European countries.

Volumes of assets under management are a key risk driver. EU/EEA AIFMs have predominantly global and European investment targets. Over half of asset classes are alternative investment, private equity or venture capital. These asset classes are typically less transparent and less liquid than traded securities and thus subject to higher ML/TF risk.

The quality and transparency of distribution channels is also an important risk factor for EU/EEA AIFM. Indeed, the relationship between the IFM and end-investors is further distanced due to cross-border management and cross-border distribution, which increases the ML/TF risks.

Non-EU/EEA AIFMs also act as designated AIFM of Luxembourg investment vehicles but are supervised by non-EU/EEA National Competent Authorities. The funds managed are typically less transparent and less liquid than traded securities and subject to higher ML/TF risk.

The quality and transparency of distribution channels is also an important risk factor for non EU/EEA AIFM. Indeed, the relationship between the IFM and end-investors is further distanced due to cross-border management and cross-border distribution which increases the ML/TF risks.

Self- or internally managed UCI

Luxembourg only has a very limited number of self-managed investment companies ("Sociétés d'investissement autogérées" or "SIAG") with relatively low assets under management and the market is very concentrated. SIAG initiators originate from nine different jurisdictions, exclusively in Europe and North America.

SIAG are self-managed UCITS investment companies (SICAV), which present lower ML/TF vulnerabilities due to the nature of their investments and regulatory restrictions. As UCITS, SIAG invest in traded securities such as bonds and equities, the transparency of which and liquidity reduces risk of abuse or misuse for ML/TF.

The internally managed alternative investment funds ("fonds d'investissement alternatifs gérés de manière interne" or "FIAAG") are composed of internally self-managed AIF. The FIAAG are initiated from a very diverse set of countries but in terms of net assets and number of sub-funds most initiators originate from Luxembourg.

Those funds appear to primarily invest in traded securities (e.g. bonds and equities), therefore reducing their ML/TF risk exposure on assets.

Regulated securitisation vehicles

Regulated securitisation vehicles are securitisation undertakings governed by the law of 22 March 2004 on securitisation that issue securities to the public on a continuous basis (more than three issues per year).

The ML/TF risks are primarily driven by the **sector size** and the **international nature of the business.** As of December 2019, in Luxembourg, there are 33 firms with a balance sheet total of €52.7 billion. In 2019, there were 378 issues with a volume of €21.9 billion, and 311 maturities/full or partial redemptions with a volume of €20.3 billion, which is not a significant change from 2016[342]. The ownership of regulated securitisation vehicles is 100% international (with 44% ownership in France, 25% in the Channel Islands, 21% in the Netherlands). Most of the clients come from the EU, but there is a non-minor share of clients from Asian markets.

The sub-sector's inherent ML/TF risk is reduced by the fact that regulated securitisation vehicles in Luxembourg are found not perform TCSP activities in practice according to CSSF data. Further, all of them are required to have their notes distributed by MIFID firms, which limits their exposure to ML/TF abuse. Also note the **complexity of ownership schemes have been reduced** over the past four years, with the value of subscribed capital falling from €4.4 million in 2016 to €2.2 million in 2019. In addition, all regulated securitisation vehicles have a Luxembourgish banking institution, providing custody for liquid assets and securities, which ensures indirect AML/CFT supervision and further limits ML/TF risk.

CSSF-supervised pension funds

CSSF-supervised pension funds which are supervised by the CSSF, are less vulnerable to ML/TF risk in Luxembourg. They are defined in the 2005 Pension Funds Law as Variable Capital Pension Savings

[342] CSSF *data*, 2019

Company (SEPCAV) and the Pensions Savings Association (ASSEP) regimes. Note that the CAA also supervises a separate type of pension types, falling under pension funds under insurance legislation, the ML/TF vulnerability of which is described in the section "CAA-supervised pension funds" of this report.

The ML/TF risk of pension funds in Luxembourg is limited because of the **small sector size,** which is also **highly concentrated**. As of 2019, there are 12 entities registered as pension funds and falling under CSSF supervision. Together, they have €1.75 billion AuM[343], and top five entities have 84% market share[344] with 18 444 clients[345].

The **international exposure is limited** as ownership by entities from foreign countries represents €0.66 billion of assets[346] in 2019. They offer **standardised products** with little ML/TF risks and have no flows with geographies weak AML/CFT measures, as most sponsors are EU-based corporates.

6.2.1.3. MVTS

Globally, money or value transfer services providers are commonly used by criminals engaging in ML/TF activities, given the international payments driven nature of the sector. In addition to the core activities performed by MVTS providers, the speed and volume of transactions and geographic reach offered are particularly attractive features, which hinder detection of suspicious activity.

Luxembourg is vulnerable to increased ML/TF risks due among other to the **volume of the sector** in the country. 2.4 billion inflow transactions worth € 93.8 billion and 1.2 billion outflow transactions worth €83.2 billion were processed by 20 entities in 2019. Note that while the number of entities increased to 20 in 2019 from 14 in 2017, it has not changed the complexity of the sector. The business models and activities of the new entrants are similar to the other actors of the sector. In addition, the international nature of the payments business increases ML/TF risks, as there is a **significant amount of cross-border** transactions involved. However, approximately 96% of the flows are within the EU. Flows to geographies with weak AML/CFT measures are limited. As such, during 2019, the inflows and outflows to and from non-EU countries represent less than 5% of the total inflows.

MVTS providers could potentially experience larger exposure to ML/TF risks stemming from an increase in online purchases as a result of the COVID-19 related social distancing measures. The increase in online purchases may lead to the increase in both the volume and value of online payments services. Further detail is provided in section 4 of the NRA on the impacts of COVID-19.

Payment institutions

Payment institutions can offer a variety of services, such as the provision of payment infrastructure (including payment accounts) to e-commerce marketplaces, peer-to-peer payment methods, facilitation of payment transactions including the transfer of funds, issuing of payment instruments or providing acquiring activities. The vulnerability of payment institutions comes from the overall features of those activities, which can facilitate fast cross-border non face-to-face transactions.

In Luxembourg, the sub-sector has a risk profile in line with the wider sector given the number and total **value of transactions** and the **large sector size**. As of December 2019, there are 12 payment institutions operating in Luxembourg, with 372 employees and €0.5 billion in revenues. 1.1 BN inflow transactions worth €55.4 billion and 1.1 billion outflow transactions worth € 55.8 billion were processed during 2019. The risk is also driven by the nature of the different payment activities and

[343] CSSF *data*, 2019
[344] CSSF *data*, 2019
[345] CSSF *data*, 2019
[346] CSSF *data*, 2019

services provided. For example, two out of the 12 active entities provide payment services, which are linked to some extent to virtual assets.

There are two new payment institutions licensed as compared to 2018. Although the sector has grown in the number of payment institutions, the sector remains **highly concentrated** with 99% of revenue generated by top five entities.

E-Money institutions

Electronic-money (e-money) institutions are institutions that issue, distribute and redeem electronic money, which is stored in electronic format mostly in e-money wallets/accounts. E-money can be accepted and used by individuals and entities other than the e-money institution itself. E-money institutions can also offer the same payment services as payment institutions, and therefore share exposure to similar ML/TF schemes, even if the risks of e-money activities and payment services are different in their nature.

In Luxembourg, the sub-sector is similar in size and activities to the payment institutions, and thus shares similar inherent vulnerability to ML/TF risk. The sub-sector is **large in size and transaction volume**. It employs 212 people and generates €0.3 billion in revenues. 1.3 billion inflow transactions worth €38.4 billion and 0.05 billion outflow transactions worth € 27.4 BN were processed during 2019. Similar to payment institutions, it is experiencing growth in Luxembourg, as the balance sheet total of electronic money institutions increased from €1.3 billion in 2017 to €1.8 billion in 2018.

The risk is reduced by the **high concentration** of the sector. Note that although the number of entities has increased from six in 2018 to eight in 2019, it has not increased the fragmentation of the market, as is the case also with payment institutions[347].

Agents and e-money distributors acting on behalf of PI/EMIs established in other European member states

Agents are money transfer intermediaries, e-money distributors on behalf of licensed and regulated MVTS processing transfers which are established in other European member states. Payment services are a common and convenient method to perform fast transfers of money across users and geographies. Payment agents typically have less information on their clients than other, more established financial institutions. However, agents are often the only persons to meet a customer face-to-face and facilitate transactions physically. Payment agents services are often used to transfer money to countries with less mature financial systems and limited access to banking services.

Agents have a **limited market size** in Luxembourg. There are 20 agents on behalf of seven payment institutions and two agents and four distributors on behalf of five electronic money institutions as of 2019[348]. Combined, they processed €316 million of inflows and €359 million of outflows in 2018, which is significantly smaller than the approximately €11.9 billion of personal remittance outflows in Luxembourg[349].

6.2.1.4. Specialised PFSs

Specialised PFSs in Luxembourg can offer a variety of activities, such as: accounting services, corporate services, domiciliation and directorship services, depositary services and transfer agency services. They can be broadly categorised into two categories: specialised PFSs providing corporate services and professional depositaries.

[347] CSSF data, 2018

[348] CSSF data, 2019

[349] Eurostat, Personal remittances statistics, November 2019

Professionals of the financial sector, such as specialised PFSs are regarded globally as exposed to ML/TF risks due to their role as gate-keepers to the financial systems. FATF guidance states that "*criminals who generate these (illegal) funds need to bring them into the legitimate financial system without raising suspicion*"[350]. Hence, specialised PFSs, in general, may be abused to achieve these ends. They may unknowingly offer various legal, accounting and other financial activities to criminals[351].

Specialised PFSs providing corporate services

Specialised PFSs providing corporate services are vulnerable primarily due to the nature of the business, which involves supporting residents and non-residents to set up corporate structures (which may be abused for ill intentions such as setting up shell companies).

In Luxembourg the ML/TF risk is driven by the fact that many specialised PFSs **offer TCSP activities**. As of December 2019, 86% of the specialised PFSs (out of a total of 104 entities) offer TCSP activities, out of which 71% also provide transfer agency services and fund administration services. TCSP activities can be offered by entities from other sub-sectors and can be particularly exposed to ML/TF activities, which are further detailed in a separate section of this NRA report below.

In Luxembourg, the sector risk is driven by the **significant size**. There are 89[352] entities[353] with 4 478 employees[354]as of December 2019 with balance sheet assets of €0.8 billion[355] and profit of €77 million[356]. The sector has a relative degree of complexity as specialised PFSs can include various licenses, each offering different services. Those licenses include registrar agents, corporate domiciliation agents, professionals providing company incorporation and management services, and family offices.

Another factor increasing ML/TF risk of specialised PFSs is the prevalence of **distribution risks**, as specialised PFSs often use third parties to enter in contact with potential clients. Moreover, the sector in Luxembourg has sophisticated professionals whose knowledge may be misused for money laundering purposes.

Professional depositaries

As of December 2019, 16% of the specialised PFS qualify as **depositaries** (some of which also hold TCSP licenses), 88% of which perform depositories services for assets other than financial instruments (15 entities) and 12% perform depositories services for financial instruments (two entities). One of the entities which performs depository services for financial instruments has obtained in 2020 a CSDR license and no longer falls in the specialised PSF category.

Professional depositaries of assets other than financial instruments are vulnerable to ML/TF risk as they act as depositaries for specialised investment funds, investment companies in risk capital and non-regulated alternative investment funds, the assets of which may be used by criminals to launder illicit proceeds.

The main risk driver for professional depositaries in Luxembourg is the large sector size. As such, as of December 2019, the 15 professional depositories of assets other than financial instruments entities

[350] Journal of Economics, Business and Management, *FATF Recommendations Related to DNFBPs on Money Laundering Assessment,* February 2015

[351] FATF guidance, *Concealment of Beneficial Ownership*, July 2018

[352] Note that of those 89 entities, 2 entities also have licenses for depositories services

[353] CSSF *data*, 2019

[354] CSSF *data,* 2019

[355] CSSF *data*, 2019

[356] CSSF *data,* 2019

have an AuM of €67.4 billion. The risk may be increased by the fact that those professionals act as depositories for non-financial assets, which may bear a higher inherent risk of ML/TF.

6.2.1.5. Support PFSs and other specialised PFSs

Support PFSs and other specialised PFSs are deemed to have a very low exposure to ML/TF activities due to the **limited financial services client interaction** and the **low-risk nature of their activitie**s (that is, support services).

Support professional service providers mainly provide back-office IT services and do not execute transactions. These include client communication agents (article 29-1 of the 1993 LSF Law), administrative agents of the financial sector (article 29-2 of the 1993 LSF Law), primary IT systems operator of the financial sector (article 29-3 of the 1993 LSF Law), secondary IT systems and communication networks operator of the financial sector (article 29-4 of the LSF), digitisation service providers (article 29-5 of the 1993 LSF Law) and e-archiving service provider (article 29-6 of the 1993 LSF Law). As of 2019, there were 74 support professional service providers operating in Luxembourg, employing 10 005 people. Of those 74 entities, 36 were client communication agents and administrative agents, and 38 were IT system operators. Two of those entities had additional agreements for digitalisation or e-archiving service provision. In the past five years the sector size remained stable with 78 entities in 2015.

Some **specialised professional service providers**, which have been included under this sector, are less exposed to ML/TF risks compared to the wider specialised PFS sector due to the nature of service provided. Moreover the current mutual savings fund is only accessible for public servants savings. Others are considered low risk as none of these exist in Luxembourg (e.g. no license is granted at present to currency exchange dealers and professionals performing securities lending). As of December 2019, this sub-sector includes six professionals performing lending operations (article 28-4 of the LSF) and two debt-recovery services providers (article 28-3 of the 1993 LSF Law) and a mutual savings fund administrator (article 28-7 of the 1993 LSF Law). The sub-sector also includes currency exchange dealers (article 28-2 of the 1993 LSF Law), professionals performing securities lending (article 28-5 of the 1993 LSF Law), of which none are present in Luxembourg and thus cannot be misused for ML/TF purposes.

6.2.1.6. Market operators

The market operators sector in Luxembourg encompasses operators of a regulated market (article 27 of the 1993 LSF Law), investment firms operating an MTF in Luxembourg (article 24-9 of the 1993 LSF Law) and investment firms operating an OTF in Luxembourg (article 24-10 of the 1993 LSF Law).

ML/TF risk for the Market Operators sector in Luxembourg is limited due to the presence of **only one market operator** in Luxembourg – the Luxembourg Stock Exchange. The Luxembourg Stock Exchange operates two trading venues, the Bourse de Luxembourg (regulated market) and the Euro MTF (multilateral trading facility). A broad range of instruments is admitted to trading on both trading venues. A majority revolves around debt securities, investments funds, warrants, GDRs, and equities. It also diversifies into contingent convertible (CoCo) bonds, Dim Sum bonds, index-linked bonds, Tier one issues, loan participation notes, Islamic bonds, etc[357].

The risk, however, is **increased by the volume of issuance activities**. It is a large stock exchange, especially for the issuance of debt instruments. The total amount of debt issued via instruments

[357] PWC, *Luxembourg Prime Location for listing*, 2014

admitted to trading on the Luxembourg Stock Exchange in 2019 was € 1 210 billion[358], representing 1 905% of the GDP of 2019.

Additionally, in line with the financial sector in Luxembourg, it is **exposed to international flows** (about 85% of the transactions executed on the trading venues of the Luxembourg Stock Exchange were executed exclusively between foreign members in 2019[359]). At the same time, the **client risk is limited**, as the exchange is open only to a small number of members who in turn are all EU regulated investment firms or banks subject to AML/CFT obligations.

The risk is further reduced by the **small volume of transactions**. The trading volume in 2019 on both trading venues operated by the Luxembourg Stock Exchange was €96.8 million in 2019, representing 0.15% of GDP[360]. The value of equity trading was €45.7 million in 2019[361]. As a result, there is very little money flowing through the exchange, which decreases ML/TF risks. In addition, the volume of trades is very low compared to the size of the global economy and in particular, the financial sector in Luxembourg. Thus, for example, if an entity trading on the Luxembourg Stock Exchange would execute multiple buys and sales of financial instruments for ML purposes, the activity would be likely noticed by the supervisor, thus preventing this theoretical ML activity from occurring.

The ML/TF is further reduced by the specifics that the Luxembourg Stock Exchange does not hold capital linked to the primary issuance of instruments traded on its markets on its accounts and does not intervene in settlement of the secondary market transactions.

[358] FESE data
[359] CSSF *data*
[360] FESE data
[361] FESE data

6.2.2. CAA supervised sectors

Globally, the insurance sector is typically regarded as less vulnerable with regards to ML/TF risks than other sectors, such as banking or gambling.[362] Insurance products are less flexible than other financial products, such as loans or payment services, limiting their attractiveness for ML/TF activities by criminals. Furthermore, insurance products are complex for ordinary criminals, requiring some specific knowledge. In addition, pay-outs from insurance companies are unpredictable and/or risky as they are dependent on the incident that has been insured actually taking place (e.g. death or tail events).

Despite this, insurance can be used by terrorists to insure their individual risks. For example, terrorists can register for life insurance policies so that the pay-out is received by their families and dependents after their death. There is also a limited risk that funds withdrawn from insurance contracts could be used to fund terrorism[363].

Insurance products are generally considered to be particularly vulnerable to ML/TF risks when they have the flexibility of payment, flexibility of investment, ease of access to accumulated funds, negotiability (i.e. can be used as collateral) and anonymity.

Flexibility of payment in insurance products may allow payment from third parties, high value premium payments and, overpayment of premia followed by refund request and cash payments. The various payment methods available may increase the attractiveness of products to criminals, as they are not limited to a specific payment scheme. The flexibility of investment enables investments in non-listed assets (for example, privately-owned companies, real estate, special purpose vehicles). As such, the inherent vulnerability of different assets may transfer to the insurer. Ease of access to accumulated funds can be provided by products with "cooling off" periods, which allow clients to cancel policies for any reason and receive a refund within a brief period of time after the policy issuance. It can also be provided by products that allow partial withdrawals/early surrender with limited fees. A criminal could potentially pay an insurance premium, and then request a refund within a short period of time to another bank account, potentially allowing for complex ML schemes. Finally, some products facilitate the anonymity of the customer, for example, by allowing deposits and payments by third parties or providing for non-face-to-face transactions (for example, mobile payment applications).

Beyond life insurance, certain features of insurance products can add to sectorial inherent risks for the insurance sector, namely, when they involve early termination, changes in beneficiaries and payments forms. Early termination includes the unexpected use of "cooling off" periods, early surrender requested within the first two years after the subscription of the policy (especially when incurring high cost) and frequent and unexplained surrenders. Changes to beneficiaries include beneficiary clause changes to an apparently unrelated third party. Payments could be further drivers of risk, for instance, when cash is used for payment, when there is a change or increase of the sum insured and/or of the premium payment, if payments are made from different bank accounts without explanation, when payment come from banks not established in the customer's country of residence or when payments are received from third parties that are not associated with the contract.

Overall, the level of vulnerability of Luxembourg's insurance sector is deemed to be medium. The sector is **significant in size and growing** with €302 billion balance sheet total[364] and €51 billion in

[362] FATF, *Guidance for a risk-based approach for the life insurance sector*, 2018

[363] FATF, *Guidance for a risk-based approach for the life insurance sector*, 2018

[364] CAA *data*, 2019. To be noted that in the context of the COVID-19 sanitary crisis, an additional time was granted to the supervised entities to communicate certain financial reporting statements to the CAA and therefore, 2019 figures are still under the process of CAA validation at the time of writing. However, the CAA estimates that even if 2019 final figures might evolve, there should be no material impact on the general conclusions inferred from those data.

premia[365] in 2019. As of 2019, it has 274[366] life insurance, non-life insurance and reinsurance companies employing over 8,000 people, about 2% of the labour force[367]. Luxembourg has one of the highest numbers of insurance companies per capita globally which significantly adds to the sectorial inherent risk. Furthermore, the sector continues to grow in Luxembourg. In 2019 compared to 2018, total value of premia written by life and non-life insurers increased by nearly a half.[368] The growth has been driven by non-life insurance undertakings, the number of which has increased as 12 entities have relocated from the UK to Luxembourg due to Brexit. This has increased the revenues of non-life insurance undertakings by more than double. In addition, premia written by life insurance undertakings increased by more than 15%, also to an extent explained by Brexit as one UK life insurance company transferred a portfolio with a value of approximately €2 BN to Luxembourg.

6.2.2.1. Life insurance

Globally, **life insurance** is the most exposed insurance sub-sector to ML/TF risks; however, the risk depends on a given product's characteristics.

Products with higher complexity or flexibility of payments, or products with returns linked to the performance of an underlying financial asset are generally more susceptible to ML/TF abuse.[369] Common money laundering techniques used in life insurance include premium payment on a policy and then asking for a refund, cashing out of policies prematurely despite penalties, funding policies using payments from a third party, paying a large top-up into an existing life insurance policy, channelling payments via offshore banks, purchasing an annuity with a lump sum rather than paying regular premia over a period of time. Life insurance policies may also be used as collateral to purchase other financial instruments, making them one part of a complex system of transactions designed to obfuscate the origins of funds[370]. Case studies 11 and 12 (below) further illustrate how the flexibility of payments and early terminations can be abused for ML purposes.

Case Study 12: Luxembourg case study on life insurance[371]

Transaction related to the purchase of life insurance

Two life insurance policies were taken out by a natural person. The premia were not paid from the account of the natural person initially indicated to the insurance company, but came from a foundation in Liechtenstein, unknown to the insurance company.

As a result of the refusal to provide supporting documents, the funds were returned to the original account and the insurance policies were cancelled.

Case Study 13: Luxembourg case study on life insurance[372]

Termination of a life insurance contract

A natural person took out a life insurance policy. The client had dual French and Canadian nationality and resided in Dubai for professional reasons. The funds were transferred from an account held in his name in France. He wished to exercise his right to renounce the contract within

[365] CAA *data*, 2019
[366] CAA *data*, 2020
[367] CAA *data*, 2019
[368] CAA, *Confirmation du développement exceptionnel du secteur de l'assurance au 4ème trimestre 2019*, 2020
[369] FATF, *Guidance for a risk-based approach: Life Insurance*, 2018
[370] IAIS, *Application Paper on Combating Money Laundering And Terrorist Financing*, 2013
[371] CRF, *Annual Report*, 2018
[372] CRF, *Annual Report*, 2018

30 days (allegedly for costs reasons) and requested the return of the funds to an account held in his name in Jersey. As the insurance company could not remove suspicions of possible tax fraud, it returned the funds to the original French account.

Life insurance products that are less susceptible to ML/TF include products such as group annuities and products that pay a lump sum or an annuity in the event of death or critical illness. Products that have no surrender value, no investment elements and products with low value also limit the attractiveness of some life insurance products for ML/TF purposes[373].

In Luxembourg, the life insurance sub-sector is **large and fragmented,** which increases its ML/TF vulnerability. As of 2019, life insurance entities show a balance sheet total of €214 billion[374], €205 billion in technical provisions[375] and €25.6 billion in premia. As of 2019, there are about 36[376] companies in the AML/CFT scope, five of which have a Luxembourgish owner. Approximately half of revenues are generated by five entities, and the share has remained stable over the past 10 years[377], which suggests the market remains structurally fragmented.

The life-insurance sector is oriented towards **foreign residents**, exposing Luxembourg to potential international ML/TF activities and high-risk customers. 92% of new premia come from foreign residents[378]. For 0.35% of all life insurance contracts, the country of residence of the policyholder is a high-risk country and for 0.44% of all life insurance contracts the banking institution from which premia originates is located in a high-risk country[379]. Life insurance entities serve a certain number of PEPs and customers from high-risk countries, as 0.2% and 0.4% of all life insurance contracts[380] have a policyholder or the beneficial owner that is linked to a PEP or a high-risk country respectively.

Other ML/TF risk factor for life insurance are the **products offered**. As described above, some life insurance products contain features increasing ML/TF vulnerability. Contracts considered as higher risk by the CAA include some local contracts[381] and freedom to provide services contracts, including life insurance policies invested in internal dedicated funds with a large part of private equity ("insurance wrappers"). As of 2019, there were 575 contracts with underlying unlisted assets[382]. Altogether, however, the number of those high-risk contracts represents less than 0.1% of total life insurance contracts. Concerning another high-risk product, the "contrat de capitalisation au porteur", after a stock-taking exercise, the CAA concluded that this product had become a rare and disappearing instrument in Luxembourg. Such contracts are not underwritten anymore and, as of the end of 2019, the 838 contracts left represent less than 0.04% of the total technical provisions of the life insurance sector.

Other ML/TF risk factors include **high volume** of transactions and the usage of intermediary **distribution** channels. In 2019, over 750 000 contracts were sold for a total premium of €19.2 billion.

[373] FATF, *Guidance for a risk-based approach for the life insurance sector*, 2018
[374] CAA *data*, 2019
[375] CAA *data*, 2019
[376] CAA *data*, 2020
[377] CAA data, 2019
[378] CAA *data*, 2019
[379] CAA *data*, 2019
[380] CAA *data*, 2019
[381] Local higher risk products are considered to mainly target investment purposes and allow a lot of flexibility regarding payments such "contrats d'épargne placement ou de capitalisation"
[382] CAA *data*, 2019

On distribution channels, direct sales are known to account for €0.6 billion. 97% (in terms of premia) were sold through intermediaries.[383]

6.2.2.2. Non-life insurance

It is globally assumed that **non-life insurance** products can be misused for ML in the case of customers paying for premia with illicit funds, or a major overpayment of premia followed by a refund request[384]. For example, in other countries cases have been observed where a company's management has exaggerated premium rates for non-life insurance products, and asked to refund some of the premia to another company owned by the management[385]. Other misuse examples include insurance fraud, when it is used to launder ML proceeds. For example, in other countries criminal organisations have insured buildings and deliberately damaged them to receive pay-outs[386].

Those approaches can also be misused for TF purposes. Another example of how TF can occur is if a worker's compensation payments are used to finance terrorist activities or purchasing primary coverage for the transport of terrorist materials[387].

In Luxembourg, non-life insurance sub-sector is **smaller and less fragmented** than the life insurance sub-sector. As of 2019, it had €39 billion in balance sheet total, €26 billion of technical provisions[388], €12.6 billion in premia and 8 284employees across roughly 42 companies (17 in the AML/CFT scope), of which three quarters had a foreign ultimate owner. The sub-sector is more concentrated with 66% of the market captured by the top five insurance firms.

It is important to note that over the past two years the non-life insurance sector has grown rapidly, and its growth has outpaced other insurance sub-sectors. The growth can be to a large extent, explained by the relocation of 11 non-life companies from the UK to Luxembourg because of the UK's decision to exit the EU. The total value of written premia almost tripled in 2019[389] compared to 2018. It was a unique event, which has not, however, changed the overall ML/TF risk of the sub-sector as most of these newcomers offer standardised non-life insurance products.

The low ML/TF risk is explained by the **low-risk nature of products**, as products offered are not inherently risky. Indeed, they pay out against pre-defined event, have no surrender value, no investment elements and the premia are generally of lower value. Moreover, insurers are especially vigilant towards fraud prevention (fraudulent claims). Insurance classes 14 (credit) and 15 (suretyship) are considered as riskier by the 2004 AML/CFT Law, however, they represent only €951 million premia in 2019.

Further, the sub-sector is **less exposed to riskier international flows** than the life insurance sub-sector. Customers are mostly international (89% of new premia from foreign countries[390]). An increasing share of turnover is realised on the markets of the EEA (82% in 2019 vs. 76% in 2018), predominantly in Germany, France and the UK, while international activity covering risks outside of the EEA is

[383] CAA *data*, 2019

[384] FATF, *Guidance for a risk-based approach: Life Insurance*, 2018 (Note: reference from page 8 for non-life insurance activities)

[385] IAIS, *Anti-money laundering and combating the financing of terrorism*, 2018

[386] IAIS, *Anti-money laundering and combating the financing of terrorism*, 2018

[387] IAIS, *Application Paper on Combating Money Laundering And Terrorist Financing*, 2013

[388] CAA *data*, 2019

[389] Confirmation du développement exceptionnel du secteur de l'assurance au 4ème trimestre 2019

[390] CAA data, 2019

experiencing a downward movement in relative terms (18% in 2019 vs. 24% in 2018).[391] For the classes 14 and 15, only four contracts were issued to PEPs in 2019, thus limiting the risk.

6.2.2.3. Reinsurance

It is often considered that reinsurance undertakings can be abused by ML/TF criminals through establishment of shell reinsurers, establishment of shell insurers to place the proceeds of crime with legitimate reinsurers or a deliberate placement by the insurer of the proceeds of crime with reinsurers to disguise the source of funds. When a criminal establishes a shell reinsurer, the following scheme may be abused: The criminal purchases a legitimate non-financial business and a reinsurer, and then purchases various esoteric risks from a legitimate insurer for the non-financial business. The shell reinsurer then reinsurers the policies issued by the legitimate insurer under a fronting arrangement, and since there is little or no insurance risk, the reinsurer earns significant profits which it can distribute to the criminal[392].

As of 2019, in Luxembourg, the sub-sector has 196 reinsurance undertakings, representing €11.4 billion in gross premia and €48 billion in balance sheet total. 91% of entities have a foreign owner and 39 companies are in the AML/CFT scope as they reinsure credit and suretyship risks.

The sub-sector includes traditional reinsurance undertakings (51 entities) and reinsurance captives (145 entities), two entity types with different product features. Traditional reinsurance undertakings provide insurance for other insurance companies wanting to limit their exposure in the event of large property damages and casualty losses. Reinsurance captives are defined by the IAIS as entities directly or indirectly created and owned by industrial, commercial or financial entities, the purpose of which is to provide reinsurance cover for risks for the entity or entities it belongs to[393].

The business of reinsurance companies is **highly international**[394] which may increase ML/TF risk. Most of the premia is written through ceding companies located in Luxembourg (5%), Germany (11%), France (14%), the UK (29%), other EEA countries (24%) and USA/Canada (7%).

The risks are, however, reduced by the **low-risk nature** of products. As reinsurance is availed by insurance companies acting as customers, the risk is lower than for life insurance undertakings. For reinsurance entities, the only ML/TF risk is the insurance customers purchase may itself bear ML/TF risk, resulting in a transfer of risk between products.

Reinsurance captives are often considered to be more exposed to ML risk than traditional reinsurance, especially in the field of tax offences. However, in Luxembourg, this risk is limited for several reasons. First, as for other reinsurance companies, the ownership undergoes close scrutiny by the regulator with regard inter alia to ML risks at the licensing process and when a shareholder change takes place. Second, reinsurance captives are fully taxable and are not subject to any special tax treatment. Third, in their on-going concern, Luxembourg reinsurance companies are required by law to set up adequate technical provisions. These technical provisions include an equalisation provision collecting every year the remaining funds after claims were paid, and thus allowing especially captives with less favourable risk diversification to cover “high risk-low frequency” exposures, (that is, where a claim does not happen every year, but once the claim happens the company may need more than an annual premium to pay for). The building up of this provision is regulated by a Grand-ducal regulation and closely monitored by the regulator on the basis of detailed business plans which must be updated regularly, thus preventing non-substantial risks to be used. The allocation to the technical provisions is tax deductible, but the reversals are fully taxable. The funds allocated to the equalization provision are

[391] CAA data, 2019

[392] IAIS, *Anti-money laundering and combating the financing of terrorism*, 2018

[393] IAIS, *Application Paper on Regulation & Supervision of Captive Insurers*, 2015

[394] CAA data

locked in and may only either serve to pay claims to the fronting company or be released into taxable results once the captive has been authorized by the regulator to give its license back. This measure has historically limited the inherent risk of this sub-sector in Luxembourg by lowering attractiveness for tax purposes[395]. Finally, the vast majority of parent companies of captives are foreign and premia come from ceding companies which are predominantly located in Europe or the UK (about 83% in 2019), limiting business with riskier geographies[396].

6.2.2.4. Intermediaries

Intermediaries include on the one side insurance agents and agencies and on the other side brokers, sub-brokers and brokerage firms. Intermediaries are deemed high risk as these businesses are retail in nature and hence tend to operate in very fragmented markets. Intermediaries are usually the first point of contact for clients and could be misused to intermediate investment of proceeds stemming from crimes such as bribery, corruption and fraud.[397] Globally, intermediaries unknowingly allowed criminals to obfuscate the beneficial ownership of insurance policies, for example, in cases when intermediaries facilitate client money transaction to insurance undertakings[398].

Further, the vulnerability of insurance product sales through intermediaries may be increased by the fact that distribution chains become long and complex and the added incentives to arrange a policy because of substantial commissions, which can be noticeably higher than for other financial products. Internationally, there have been cases where criminals used insurance intermediaries from more than five countries to limit the traceability of financial flows[399].

Luxembourg's ML/TF risks of the intermediaries sub-sector are increased by the **size and the fragmentation** of the market. There are 346 agencies, 8 353 agents, 120 brokerage firms working through 165 approved managers and 478 sub-brokers as of 2019[400].

Insurance agencies and agents are inherently less risky, as they may only be approved on behalf of Luxembourg insurance undertakings or Luxembourg branches of non-Luxembourg undertakings[401].

The risk is increased by the **high volume of transactions** in brokerage business. The new premia flow in 2019 is €65 million for non-life and €2.08 billion for life with the total premia amounting to €2.73 billion for the year.[402] The risk is also increased by the **high international nature** of the business. As such, brokers have mainly international clients (81% of premia from foreign countries for life and 76% non-life) mostly focused on the EEA and UK market (premia with non-EEA and non-UK countries accounts only for 7% in life and 12% in non-life).

6.2.2.5. Professionals of the insurance sector (PSA)

Professionals of the insurance sector (PSA) include authorised service providers of corporate governance and management companies for insurance and pension funds[403]. They typically do not manipulate money flows and play an advisory role to the respective insurance undertakings on pension funds, and thus have limited exposure to ML/TF risk.

[395] CAA *data*
[396] CAA *data*, 2019
[397] FSA, *Anti-bribery and corruption in commercial insurance broking*, May 2010
[398] IAIS, *Examples of money laundering and suspicious transactions involving insurance*, 2004
[399] MONEYVAL, *Money laundering through private pension funds and the insurance sector*, 2010
[400] CAA *data*, 2019
[401] 2015 Insurance Law, article 284-2, para 1, subpara 2, 2nd sentence
[402] CAA *data*, 2019
[403] CAA *website*

The **small sub-sector size** of the professionals of the insurance sector further limits ML/TF exposure. In Luxembourg, in 2019 they generated total revenues of €52 million with 25 PSA entities (for a total of 35 licenses). Of the 35 licenses, 20 licenses were for management companies of insurance, captive insurance, reinsurance undertakings or pension funds, three were for management companies of insurance portfolios, nine for authorised providers of actuarial or governance-related services, and three for claim handlers. Five management companies of captive insurance and reinsurance have a license to act as domiciliary agent. Note that the domiciled companies are mainly entities supervised by the CAA or linked to entities supervised by the CAA (for example, companies pertaining to the same group).

PSAs are all locally licensed but **seldom owned by foreign entities**, and **do not have international business**, which further reduces their ML/TF vulnerability.

6.2.2.6. CAA-supervised pension funds

CAA-supervised pension funds, similar to the pension funds supervised by the CSSF, are less vulnerable to ML/TF risk in Luxembourg than other CAA-supervised entities. The CAA-supervised pension funds are defined under the 2015 Insurance Law in Article 32(1) point 14. They are similar to CSSF-supervised ASSEP pension funds, in that they also offer defined benefit, cash-balance and defined contribution schemes, and that affiliated members are creditors of the pension fund.

While pension funds are considered to have an inherently lower ML/TF vulnerability, some pension funds globally can be structured similarly to life insurance products. They may, in rare cases, offer cancellations or early redemptions, features that can increase ML/TF risk. In addition, criminal proceeds can be invested into pension funds as both long-term investments and shelter of funds from confiscation[404].

In Luxembourg, the ML/TF risk is limited due the **very small sector size.** As of 2019, there were three CAA-supervised pension funds with €82 million revenues and €539 million in balance sheet total. The small sector size and the **low fragmentation** make the sector highly transparent, and acts as a barrier for criminals to abuse the sectors. Furthermore, the **low-risk products** offered by the pension funds reduce the overall ML/TF vulnerability of pension funds to a low level.

[404] MONEYVAL, *Money laundering through private pension funds and the insurance sector*, 2010

6.2.3. Legal professions, chartered accountants, auditors, accountants and tax advisors

Table 15 below summarises these professions in Luxembourg and their respective supervisor for AML/CFT purposes. It should be noted that the auditors, chartered accountants, notaries, lawyers and bailiffs are self-regulated professions in Luxembourg, and hence are supervised for AML/CFT purposes by their respective self-regulatory body ("SRB"). In turn, accountants and tax advisors are unregulated professions but under the supervision of AED for AML/CFT purposes.

Table 15: Luxembourg legal professions, accountants, auditors and tax advisors and their respective supervisor for AML/CFT purposes

Profession	Term in French	Term in English	AML/CFT Supervisor/SRB	Acronym
Regulated professions (including for AML/CFT purposes)				
Auditors	Cabinets de révision	Audit firms	Institut des Réviseurs d'Entreprises	IRE[405]
	Cabinets de révision agréés	Approved audit firms		
	Réviseurs d'Entreprises	Statutory auditors[406]		
	Réviseurs d'Entreprises Agréés	Approved statutory auditors		
Chartered accountants	Experts-comptables	Chartered professional accountants[407]	Ordre des Experts Comptables	OEC
Notaries	Notaires	Notaries	Chambre des Notaires	CdN
Lawyers	Avocats	Lawyers	Ordre des avocats du Barreau de Luxembourg	OAL
			Ordre des avocats du Barreau de Diekirch	OAD
Bailiffs	Huissiers de justice	Court bailiffs and judicial officers	Chambre des Huissiers	CdH
Nonregulated professions (but supervised for AML/CFT purposes)				
Accountants	Professionnels de la comptabilité	Accounting professionals	Administration de l'Enregistrement et des Domaines	AED
Tax advisors	Persons other than those listed above who exercise in Luxembourg, by way of their business, an activity of tax advice or one of the activities described in point (12)(a) and (b), and any other person that undertakes to provide, directly or by means of	Tax advisors	Administration de l'Enregistrement et des Domaines[409]	AED

[405] CSSF is the independent Public Oversight body of the Audit Profession and is responsible for performing market entry controls

[406] Note that statutory auditors, approved statutory auditors, audit firms and approved audit firms may also be chartered professional accountants. The [approved] statutory auditors and the chartered professional accountans are two different accreditations

[407] Note that chartered professional accountants can also be statutory auditors, approved statutory auditors, audit firms and approved audit firms. The [approved] statutory auditors and the chartered professional accountans are two different accreditations

[409] If the tax advisor is a member of a SRB, then the professional is supervised for AML/FT purposes by the respective SRB. If this is not the case, the professional is supervised for AML/CFT purposes by AED

Profession	Term in French	Term in English	AML/CFT Supervisor/SRB	Acronym
	other persons to which it is related, material aid, assistance or advice on tax matters as principal business or professional activity.[408]			

In Luxembourg, legal professions, chartered accountants, auditors, accountants and tax advisors are also exposed to ML/TF risks, due to similar risk drivers as in other jurisdictions such as their legal status key role as intermediaries. There is a significant number of professionals i.e. 2 917 lawyers[410]; ~1 170 chartered professional accountants[411] spread across 558 legal entities and 58 independent professionals, 581 statutory auditors and approved statutory auditors and 78 audit firms and approved audit firms[412]; 395 accounting professionals and tax advisors[413]; 36 notaries[414] and 19 court bailiffs [415] as well as eight deputising bailiffs[416]. These professionals serve a wide range of clients and international businesses.

Additionally, some of these professionals enable the creation and management of complex legal structures and arrangements which are witnessed to be commonly used for ML/TF purposes. These apply to different professions to different degrees (for instance, notaries legally required to register real transactions but do not provide financial services; bailiffs also do not have a role in financial services, etc.).

Even though their core activities are not inherently risky, their ability (except notaries and bailiffs) to provide TCSP services in addition to their core activities exposes them to higher risk[417].

6.2.3.1. Auditors[418]

The auditors consists of audit firms, approved audit firms, statutory auditors and approved statutory auditors. Table 16 below provides an overview of the auditors landscape in Luxembourg.

Table 16: Overview of the auditors landscape in Luxembourg

Entity / professional	Luxembourg name	Total number in Luxembourg in February 2020
Audit firms	Cabinets de révision	23

[408] Referring to the 2004 AML/CFT Law, Article 2 (1), Paragraph 13

[410] "Ordre des Avocats du Luxembourg" and "Ordre des Avocats de Diekirch", *data submitted (as of 31st December 2019)*

[411] "Ordre des Experts Comptables" *data submitted (as of 31st December 2019)*

[412] "Institut des Réviseurs d'Entreprises" *data submitted (as of February 2020)*

[413] Referring to those accounting professionals and tax advisors that are not a member of the SRB and are supervised for AML/CFT purposes by the AED

[414] Number fixed by law; see *"*Règlement grand-ducal modifié du 17 août 1994 ayant pour objet de déterminer le nombre et la résidence des notaires*"* (link)

[415] Number fixed by law; see *"*Règlement grand-ducal du 25 septembre 2009 concernant le nombre et la résidence des huissiers de justice*"* (link)

[416] The maximum number (10) is fixed by law; see *"*Règlement grand-ducal du 4 février 2016 concernant le nombre des huissiers de justice suppléants*"* (link)

[417] The section "Cross-cutting vulnerabilitites – TCSPs" provides more detail on TCSP activities. See also "Trust And Company Service Providers – Guidance for a risk based approach", June 2019, FATF

[418] In this document, the term "audit profession" covers equally the statutory auditors ("Réviseurs d'Entreprises"), the approved statutory auditors ("Réviseurs d'Entreprises Agréés"), audit firms ("Cabinets de Révision") and approved audit firms ("Cabinets de Révision Agréés").

Approved audit firms	Cabinets de révision agréés	55
Statutory auditors	Réviseurs d'entreprises	261 presented as follows: • 148 in public practice • 113 in business[419]
Approved statutory auditors	Réviseurs d'entreprises agréés	320

For the audit profession, exposure to ML/TF risks is due to three main reasons. First, in Luxembourg, **auditors is sizable and moderately fragmented profession**, with 581 professionals (statutory auditors and approved statutory auditors) in total out of which 468 are working in 78 audit firms and approved audit firms or as a sole practitioner, as of February 2020. The five largest audit firms account for 73% of statutory auditors and approved statutory auditors (345 out of 468 professionals in public practice). The remaining 27% (123) professionals are employed by 73 audit firms, with nine professionals working as sole practitioners.

Secondly, **auditors' activities expose them to being misused or abused for ML/TF purposes.** A core activity of the audit profession is auditing and validating the annual accounts of its customers. The audit profession has unique access to its clients' financial history. But statutory auditors are usually one step removed from the daily client accounts which might limit the visibility. As such, they can play a key role in identifying ML/TF activities but are also prone to misuse or abuse for ML/TF purposes[420]. In addition, audit professionals perform TCSP activities which are considered as particularly ML/TF high risk by FATF[421]. It should be noted that most activities performed by the audit profession, such as assurance services, are believed to be low-risk for AML/CFT purposes, whilst activities such as TCSP activities are deemed higher risk. As of the first semester 2020 however, data are being assessed to determine higher risk and lower risk activities and hence a conservative approach is taken in line with the NRA methodology.

Finally, **the 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.

The case study (below) illustrates how the audit profession could be abused or misused for ML/TF.

Case Study 14: Financial irregularities, forgery and use of forgeries committed by one of the companies in which a specialised investment fund (SIF) had invested[422]

One of the companies in which the SIF in question had invested is currently in judicial liquidation. This investment was made in February 2016 on the basis of:

- Legal and financial due diligence reports that did not mention any significant issues;
- The audited accounts that were issued by the auditor for the past four years.

In August 2016, the CEO of this company died unexpectedly and a consultant was hired to assist in the management of the business. A forensic accounting firm was also appointed for financial audits and, in November 2016, it found that financial irregularities had occurred. External legal advisors were appointed and their analysis revealed that irregular acts were committed by the production and use of forged documents, in particular in conjunction with the senior management of the time, including the deceased CEO.

[419] Out of which, more than 40 are employed by the "Commission de Surveillance du Secteur Financier" as of February 2020.

[420] See, for instance, "Trust And Company Service Providers – Guidance for a risk based approach", June 2019, FATF

[421] The section "Cross-cutting vulnerabilitites – TCSPs" provides more detail on TCSP activities

[422] Case study taken from CRF Annual Report 2018

In light of the above, the vulnerability of auditors is considered high, considering their ability to provide TCSP services in addition to their core activities.

6.2.3.2. Accounting profession: Chartered accountants ("Experts-comptables")

In Luxembourg, chartered accountants are a **large and fragmented profession**, with 1 173 chartered accountants spread across 558 legal entities and 58 independent professionals as of May 2020. A significant portion of the chartered professional accountants is part of one of the six largest firms; 388 of the professionals are employed by one of the Big 4 firms or assimilated legal entities, which amounts to 33%[423]. The rest of the profession is spread across the remaining legal entities or are independent professionals. Tables 17 and 18 (below) illustrate that the entities under OEC supervision are mainly very small legal entities and independent professionals (more than 75% entities have under 10 employees) and have a limited revenue (56.2% have a revenue of less than € 500 000).

Table 17: Distribution of entities under OEC supervision per size (as of 31 December 2018) [424]

	Number of employees[425]				
	< 10	10-29	30-49	50-249	> 250
Percentage of entities	77.5%	13.8%	3.7%	3.7%	1.4%

Table 18: Revenue range of entities under OEC supervision (as of 31 December 2018) [426]

	Revenue range				
	< 500k€	500k – 1m€	1-10m€	10-100m€	> 200 m€
Percentage of entities	56.2%	16.5%	24.1%	2.3%	0.9%

Chartered accountants provide a **key gatekeeper and intermediary role for many transactions that have a high risk for ML/TF**. In addition, they perform TCSP activities which are considered as particularly ML/TF high risk by FATF[427]. These represent a significant proportion of their activities. As shown in Table 19 (below), 60% of chartered accountants (legal entities and independent professionals) under OEC supervision provide domiciliation services; 14% indicate that more than 75% of their revenues originate from domiciliation activities. TCSP services are considered as high risk from an ML/TF perspective. Other activities of chartered accountants such as tax and administrative advice and establishment of annual accounts are prone to misuse or abuse for ML/TF purposes, though the level of ML/TF risks is likely lower.

[423] "Ordre des Experts-Comptables" *data submitted (as of 31st December 2019)*

[424] Data has been collected through the 2019 RBA questionnaire (data received May 2020)

[425] The size of an entity is expressed according to its number of employees, including "experts-comptables" and "non experts-comptables". Entities include legal entities and independent professionals

[426] Data has been collected through the 2019 RBA questionnaire (data received May 2020)

[427] The section "Cross-cutting vulnerabilitites – TCSPs" provides more detail on TCSP activities

Table 19: Activities performed by OEC legal entities / independent professionals and percentage of total revenue stemming from this activity (TCSP activities in green) [428]

		percentage of total revenue			
Activities	**% professionals performing this activity**	**> 75%**	**10-75%**	**< 10%**	**Not significant / not applicable**
Comptabilité / Accountancy	84%	14%	78%	5%	3%
Conseil fiscal - déclarations fiscales / Tax advice - tax returns	81%	3%	54%	33%	10%
Domiciliation / Domiciliation	60%	2%	36%	43%	18%
Secrétariat social / Corporate secretary	50%	*n/a*	42%	42%	16%
Mandat d'administrateur / Director's mandate	49%	2%	30%	37%	31%
Dépositaire de titres au porteur / Custodian of bearer shares	27%	*n/a*	4%	6%	91%
Location de bureau / business center / Office rental/ business center	25%	*n/a*	14%	42%	44%
Autres / Others	25%	16%	52%	26%	6%
Conseil fiscal - structuration fiscale / Tax advice - tax structuring	26%	3%	20%	42%	36%
Mandat de liquidateur / Mandate as liquidator	22%	*n/a*	7%	34%	59%
Activité de conseil en organisation / Organizational consultancy activity	18%	4%	30%	33%	33%
Contrat fiducie / Fiduciary contracts	5%	*n/a*	35%	*n/a*	65%
Actionnaire Nominee (portage d'actions) / Nominee Shareholder	4%	*n/a*	11%	*n/a*	89%

In light of the above, the vulnerability of chartered accountants is considered high, considering their ability to provide TCSP services in addition to their core activities.

6.2.3.3. Notaries

Even though there are only 36 notaries in Luxembourg, **the notaries employ a larger number of professionals**: approximately 250 to 300 professionals in 2019. This typically includes 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. In 2018 and 2019, five new notaries were appointed (mostly due to retirements and changes in offices); four notaries in office changed office (the total number of 36 notaries are capped by law), and in 2020-2021, further new notaries will be appointed given expected further retirements.

Notaries are gatekeepers to many business acts[429] (such as legal entity set-up, mergers, sale of business and credit opening) and real estate transactions. Several of the activities performed by

[428] Data has been collected through the 2019 RBA questionnaire (data received May 2020)

[429] Some legal entities / arrangements are out of scope for notaries (e.g. some "fonds d'investissement alternatif réservé" (FIAR) and "SARL Simplifiée"); only acts requiring changing articles of incorporation require notaries

notaries are marked as particularly high risk by the FATF, such as overseeing real estate transactions, the purchase of shares or other participations, legitimisation of identities of signatory, legalisation of old documents[430] or opening of safe deposit boxes in the framework of successions or divorce procedures[431,432]. In 2019, notaries in aggregate were responsible for guaranteeing the legal formalities and feasibilities of around 29 600 real estate related transactions[433]. Despite representing a significant share of notaries' activity, it should be noted not all such real estate deeds entail a monetary consideration (i.e. some of these deeds are related to successions, donations, wills, parental partition *inter vivos* and marital agreements). Notaries are also authorised to conduct real estate public auctions for which they have an exclusive mandate, though this is estimated to be a small share of notaries' overall activities (no more than 50 auctions per year on average). Additionally, notaries have an important role in accessing and updating existing company registers: they provide some information to the RCS by means of their relevant company law deed and must consult and inform the LBR if they detect a mismatch between the registered beneficial owner and the information that the client has provided them with.

Some of Luxembourg notaries are involved in business acts with a wide variety of clients and international businesses, due to the nature of Luxembourg's financial centre and its diverse resident and working population. However, it has been observed by notaries that the majority of the 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. Newly appointed notaries usually start building their clientele amongst local private individuals and local SMEs. Deeds set up for private individuals and SMEs do not usually concern businesses, which are particularly exposed to ML risks. This is most notably the case for the majority of deeds related to family or general civil law subjects, such as the setting up of wills, marriage contracts, succession planning or real estate transactions carried out for residential purposes.

Non-face-to-face business interactions are extremely rare with natural persons but in certain cases with legal entities could be made via intermediaries, which may, depending on the particular case, increase the ML/TF risk (i.e. contact mostly with lawyers and not always ultimate customers).

Notaries are set up as *"profession libérale"* and act as *"personnes physiques"*. This means that they are not set up as companies or partnerships and **no external ownership exists**. All 36 notaries are Luxembourg nationals. Previously it was a requirement by law that notaries appointed were Luxembourg nationals; this has changed in recent law so new appointees' nationality mix may change in the future.

Case Study 15: Nomination of an alleged mafioso as managing administrator of a private limited liability company (SARL) despite his criminal background (2019) [434]

An alleged mafioso was nominated as managing administrator of a small private limited liability company (SARL). This person was nominated without a notarised deed, which means that his name was added in a small statute change after the creation of the SARL; the notary himself was not implied in these changes.

[430] Both legitimisation of identities of signatory and legalisation of old documents are very rare in Luxembourg

[431] Opening of safe deposit boxes may occur in the framework of successions or divorce procedures and is very rare in Luxembourg.

[432] International standards on combating money laundering and the financing of terrorism & proliferation – FATF recommendations

[433] Data from AED, August2020. At present, a more granular breakdown of notaries' activities is not available, to determine which acts relate to real estate transactions with a monetary consideration and which do not.

[434] Source: "Santo Rumbo case shows the flaws in fight against money laundering"; News item on 28th August 2019 at RTL Today (https://today.rtl.lu/news/luxembourg/a/1395392.html)

When preparing such deeds, notaries check the identity of the beneficial owner. Other names listed in a deed – especially in terms of small businesses, as it was the case here – are checked on a risk assessment basis which also takes into account whether the persons in question are personally known to the notary. Concerning this specific case, the case was reported in the local news in August 2019 and brought to the attention of the President of the CdN, who conducted the necessary investigations and reported the findings to the CdN Committee. No professional shortcomings were detected on the side of the notary profession, but the case highlights how company registration can expose notaries to ML/TF risks.

In light of the above, the vulnerability of notaries is considered high.

6.2.3.4. Lawyers

Lawyers are vulnerable to ML/TF due to three main reasons. First, in Luxembourg lawyers are a **large and fragmented profession**, with 2 917 lawyers working across 557 law firms as of April 2020. OAL supervises 2 868 professionals operating in 529 different law firms, with ~30% of lawyers employed by the seven largest law firms and a long tail of small firms (397 law firms with less than 10 lawyers; 197 with one lawyer). OAD supervises 49 professionals operating in 29 different law firms, all rather small (18 of them are single-lawyer firms) with the largest law firm having about seven lawyers. Most law firms are owned or controlled by Luxembourgish beneficial owners with 117 entities (~20%) owned or controlled by foreign owners of which 116 are based in the EU. Regardless, the high fragmentation of the sector increases the ML/TF risk. In aggregate, lawyers' revenues are significant, also given that Luxembourg is a large financial centre and a significant share of lawyers' business is likely to originate from the financial sector. Besides that, approximately 60% of the OAL lawyers that responded to the first questionnaire[435] state they perform activities that fall in the scope of the 2004 AML/CFT law, which amounts to about 1 400 lawyers.

Secondly, lawyers provide an important role as **gatekeeper and intermediary for various transactions with a high risk for money laundering**. They possess relevant legal expertise, offer a variety of different services to their clients and typically have favourable (often significant) external credibility from their professional status. The range of lawyers' activities has not undergone a major change in the past two years. Services 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, and the actual setting up and operation of, corporate structures and other legal arrangements for clients (including domiciliation). Importantly, some of these activities performed by lawyers are deemed as TCSP services[436], which are considered particularly high-risk for ML/TF purposes as per FATF guidance. Approximately one third of the OAL lawyers that responded to the first questionnaire state they perform TCSP services *(see also the section "cross-cutting vulnerabilities – TSCP"' for more detail)*. The OAL has determined based on inspections performed that, generally speaking, 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

[435] ~75% of the 2,868 lawyers registered in Luxembourg responded to the questionnaire

[436] Namely, as per 2004 AML/CFT Law: 1) Acting as a formation agent of legal persons; 2) Acting (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; 3) Providing a registered office, business-, correspondence- or administrative address for a company, a partnership or any other legal person or arrangement; 4) Acting as (or arranging another person to act as) a fiduciary of a *fiducie* or other similar legal structure; 5) Acting as (or arranging for another person to act as) a nominee shareholder for another person.

and lawyers practicing on an individual basis mainly practice activities relating to litigation[437]. It should be noted that OAD lawyers' activities are mostly oriented towards litigation. As with OAL, whilst no objective estimate exists today on the distribution of activities, further clarity on this for OAD (including the share of potential TCSP activities for OAD lawyers) is expected when the OAD sends a questionnaire to its members, which it plans to do in 2020.

Case Study 16: Potential financial misappropriation (2019)[438]

In December 2018, Firm A (the "Firm") was contacted by a foreign state wishing to receive legal assistance and advice in relation to a transaction involving a property located in London (the "Property") owned indirectly by a Jersey-registered company (the "Target"), itself owned by a Luxembourg SA, whose director and beneficial owner would appear to be Mr F. Following lengthy discussions and negotiations, on 2 May 2019, the foreign state acquired the Target's securities, thereby indirectly becoming the sole and exclusive owner of the Property. The agreement also provided that the foreign state would sell the shares it held in the Seller's capital to Mr F.

In the course of routine KYC checks, the Firm discovered the following corroborating facts reported by the Italian press and later by the international press. A scandal is said to have rocked the foreign state. Gifts had reportedly been invested in luxury properties, including the purchase of the freehold to a luxury apartment block in the heart of central London. Financial arrangements are said to have been put in place via Switzerland and Luxembourg as regards the financial management of this property.

The press reports that this financial management, which was not particularly advantageous for the foreign state, prompted it to buy back the entire block located in London. At the time of the purchase, the foreign state allegedly acquired units in a Luxembourg fund B managed by the holding company of businessman G. He is said to have made a sizeable capital gain by selling his own units to Mr F and his Luxembourg SA, making them business partners and co-owners with the foreign state. In total, the foreign state is said to have invested €200 million in the management and refurbishment of the Property. Following a report by the foreign state's asset administrator, the foreign state's court of auditors (which audits the foreign state's accounts) is said to have taken the matter to court and an investigation has been launched into financial misappropriation. Five people are reported to have been implicated, including the head of the financial administration in the foreign state.

Finally, lawyers serve a **wide range of clients and international business**, with a wide diversity of non-resident clients and transactions in Luxembourg. There has been limited change in the client base of lawyers in the past two years. Clients are sometimes acquired via intermediaries and non-face-to-face interaction can occur.

In light of the above, the vulnerability of lawyers is considered high, considering their ability to provide TCSP services in addition to their core activities.

6.2.3.5. Court bailiffs

"Huissiers de justice" (court bailiffs) are appointed by the Grand Duke and are ministerial officers with the sole competence to serve judicial documents and to proceed to the enforcement of court decisions. Court bailiffs nevertheless operate as practitioners of an independent self-employed

[437] In general the OAL estimates that approximately 50% of the lawyers registered with the Bar are practicing activities in scope of the AML Law.

[438] Case study provided by OAL on 1st July 2020, based on an STR dated 15 November 2019

profession, regulated by the self-regulated body *Chambre des Huissiers*. They engage in diverse legal missions such as collecting debt, signing legal acts and more.

The sector is **relatively small** (19 court bailiffs and 8 deputizing court bailiffs in Luxembourg).

They pose some ML/TF risks, in particular in their **capacity as gatekeepers for private auctions**[439] (i.e. organizing public sales of furniture, household effects and harvests). The number of auctions (~60 per year) and the number of court bailiffs carrying out auctions (~12 out of 19) are relatively low. Moreover, only a few auctions per year are voluntary auctions by individuals or companies, with the remaining ones being forced auctions (following a legal decision) or auctions following a bankruptcy. The amounts of money typically involved in those auctions is low as well, even though in exceptional cases mostly related to involuntary bankruptcy, a batch may include goods tendered valued above €5 000 (e.g. construction vehicles and machines). Nonetheless, the value of some auctions can be considerable. In 2019, "huissiers de justice" completed 60 auctions, where 683 items have been sold for a total amount of €1 011 252 (average €18 854/auction and 1 480/item) and prices per item ranging from €1 to €70 000.

Besides overseeing auctions, court bailiffs also have other legal missions, with lower ML/TF risk, such as the execution of legal decisions on Luxembourg residents (e.g. debt collections, eviction orders, service of acts and exploits, make purely material findings). It should be noted that court bailiffs do not accept cash for large amounts (above €15 000).

In n light of the above, the vulnerability of bailiffs is considered medium

6.2.3.6. Accountants and tax advisors (supervised by AED)

In Luxembourg, the sub-sector's vulnerability is also increased by to the **large sector size**. As of 2019, there were 395[440] accountants and tax advisors. Further, the large component of **international business involved** (10 times higher import and export of auditing services in Luxembourg than peers[441]) also exposes the sub-sector to international flows, that may lead to ML/TF misuses.

Accountants and tax advisors[442] can offer a variety of services that can be potentially misused by criminals for laundering illicit money. Accountants, for example, although they cannot certify accounts like chartered accountants, they can be abused in their activity of recording accounting entries to record entries related to money laundering. Also, although the Domiciliation Law prohibits them to provide domiciliation services, they may, however, provide other TCSP services that are not reserved for professionals. Tax advisors advise clients on taxes, and thus be misused to facilitate tax evasion and VAT fraud[443].

In Luxembourg, in line with global activity typologies, the **specifics of the activities** of accountants and tax advisors may drive ML/TF risk. As such, the proprietary knowledge they possess may be misused for unlawful activities.

In light of the above, the vulnerability of accountants and tax advisors is considered high, considering their ability to provide some TCSP services in addition to their core activities.

[439] This excludes real estate auctions, which are overseen only by notaries (in fact, notaries in Luxembourg can do both real estate and non-real estate auctions)

[440] Includes tax advisors, total unknown

[441] UN *Comtrade* 2015 figures

[442] As per the table (above) this concerns accounting professionals and tax advisors supervised by AED

[443] FATF, *Risk-based approach guidance for the accounting profession,* 2019

6.2.3.7. Trust and company service providers ("Prestataires de services aux sociétés et fiducies" (TCSPs)

The TCSP category includes in itself business centres and directors, which are professions that are both supervised by the AED[444]. Based on the 2004 AML/CFT 2004 law, business centres are allowed to provide a registered office, business, correspondence or administrative address for a company, a partnership or any other legal person or arrangement. For business centres, the entities have to meet two conditions: provide domicile, and "services liés" (related services), which may include a variety of activities, such as reception service, telephone service, provision of equipment such as a printer, postal mail delivery or Wi-Fi. Accordingly, any natural or legal person can act (or arrange for another person to act as) as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons.

The ML/TF risk for the sub-sector is primarily driven by the nature of TCSP **activities, which are identified as high risk**. The detailed assessment on TCSP-related risks are provided in the section "TCSP activities" of the NRA. In addition to the product risk, the **sub-sector's size and large fragmentation** may drive ML/TF risk. As of 2019, there are 661 directors (natural persons) registered for VAT purposes with the AED. There are at least 100 business centres operational in Luxembourg. In addition, business centres may register companies that do not have physical presence at the centres, and as such have limited visibility on its activity.

[444] Professionals who perform these TCSP services that are a member of a SRB are not supervised by AED but by the respective SRB

6.2.4. Gambling

Gambling is generally regarded as particularly vulnerable to money laundering given the high volume of transactions and the widespread usage of cash to purchase tickets and to cash out winnings[445]. Additionally, the emergence of online gambling websites provides additional anonymity, further increasing the lure of this sector for ML purposes.

In Luxembourg, the gambling sector is however limited and mostly concentrated around three activities: one casino, the National Lottery and ad hoc lotteries. There are no authorised domestic online gambling companies or sports betting firms at the time of the drafting of this document. Online sports betting cannot be authorised according to the 1987 Sports Betting Regulation, and offline sports/horse betting is only offered by the National Lottery[446]. Online gambling is not permitted; so no legal online gambling companies operate domestically.

6.2.4.1. Casinos

Globally, **casinos** are typically considered as particularly vulnerable to a wide range of money laundering techniques, given the wide customer base and large sums involved. Further, the ML risk is increased as most transactions are cash-based. For example, 80% of payments in some European casinos are undertaken in cash[447]. Some global examples on how casinos can be misused for ML/TF include refining, by which launderers pay low denomination cash into their casino accounts and withdraw funds with cash of higher denomination, and criminals buying chips for cash and then redeeming value through money transfer. Casinos are often targets of organised crime groups, and there have been cases internationally where employees of casinos became complicit in ML/TF activities. For example, employees can falsify player ratings and other gambling records to justify the accumulation of casino chips, and make detection of a criminal harder to catch[448].

In Luxembourg, the **size of the sector is very small**, which limits the inherent ML/TF risk. Luxembourg's privately owned and only casino (Casino 2000) had 435 000 visitors in 2019[449], 200 employees[450] and total revenues of €53 million (of which €46 million gambling revenues, "GGR"[451]). About 5% of total gambling revenues are accounted for by table games (Black Jack and Roulette) and ~95% of GGR from slot machines. The low volumes mean that vulnerability to ML/TF is limited compared to other sectors in Luxembourg and the gambling sector in other countries.

The ML/TF vulnerability is further reduced by the fact that the casino's **clientele is regular and regional**: 28% of the casino customers are from Luxembourg and 60% from France, mainly within a radius of 60 kilometres from the casino. Approximately 4% of clients come from Germany and 4% from Belgium. Approximately 30% of the gambling revenues in the casino can be attributed to the highest 600 spenders. Many people visit the casino for its entertainment offers beyond gambling (for example, concerts and restaurants). The average yearly income in Luxembourg is very high so that casino customers have a higher spending power than other regional casinos. Note that all gambling activities

[445] FATF, *Vulnerabilities of Casinos and Gaming Sector*, 2009

[446] PMU for horse betting, Oddset for sports betting

[447] European Casino Association, *Response to European Commission public consultation on EU initiative on restrictions on payments in cash*, 2017

[448] FATF, *Vulnerabilities of Casinos and Gaming Sector*, 2009

[449] A total of 475 000 visitors came to the Casino 2000 Entertainment Centre, but only 435k entered the casino area.

[450] Casino 2000, *Dossier De Presse*, 2016

[451] In terms of Gross Gaming Revenues (GGR), i.e. the amount the casino keeps from all wagers minus winnings and before tax. On slot machines, customers on average lose 6% in every bet, thus bet on average ~17 times the ~€46 million GGR, generated by a total turnover of ~€780 million (i.e. 17 x €46 million) in gambling via the casino, since intermediate winnings are often replayed by customers in new bets. The amount that customers bring to the casino, in cash or via credit cards, is estimated to around five times the GGR (~€230 million), including former winnings that are brought back.

require **face-to-face interaction** with casino staff, which makes it less attractive for criminals for ML/TF purposes.

6.2.4.2. National lottery

While globally large-scales lotteries are considered less vulnerable to ML/TF risk than casinos, there have been cases in other jurisdictions where they have been abused by criminals to launder money. For example, criminals can buy winning lottery tickets from legitimate customers[452], or a retailer may offer national lottery products to be exploited for criminal purposes[453]. Lotteries may also be misused for criminals to remain anonymous, for example by using fraudulent or stolen identities when claiming significant prizes[454].

The ML/TF risk of the **National Lottery** is very limited because of **public ownership**[455]. The National Lottery is operated by the *"Œuvre Nationale de Secours Grande-Duchesse Charlotte",* which is an *"établissement public"* (public entity) under a law of 22nd May 2009[456], and managed by a dedicated general manager and the management team. Its profits are redistributed to charities in various fields (e.g. healthcare or culture) through the "*Œuvre Nationale de Secours Grande-Duchesse Charlotte"*. The "*Œuvre Nationale"* manages the annual profits generated by the National Lottery.

The ML/TF risk is further reduced by the **small sub-sector size**. As of April 2020, no other gambling or sports betting operator expect the National Lottery is authorized in Luxembourg, it has a "*de facto*" monopoly over a number of betting activities in Luxembourg. The National Lottery counted ~49 employees in 2019 exclusively dedicated to its operation. It has an average revenue of €47 million per year[457].

The National Lottery also has the majority of its revenue generated from **low-risk products**. Most (~96%) of the revenues are generated by jackpot-driven games (with a very low probability of winning high stakes) and only ~4% of its revenues coming from horse/sports betting[458] (which presents higher vulnerability given higher odds of winning lower amounts)[459]. Note that horse/sports betting have a smaller base with up to 10 000 players, where jackpot-driven games have an average of 50 000 players. Within jackpot-type games, around 79% of revenues come from draw based games (classic lotteries such as Euromillions and Lotto) and 18% from instant games (as scratch-cards). The relatively small revenues are also spread across a very broad customer base, with 35 000-50 000 regular customers on average weeks (which can go up to 80 000–90 000 customers in busy weeks).

The vast majority of customers are from Luxembourg or neighbouring countries, as **sales are limited to the Luxembourg territory**. For its draw-based games, the National Lottery has established collaborations with foreign/international lotteries (e.g. Euro Millions, Lotto), in order to offer larger potential winning pools to its customers. The instant games (in the form of scratch-cards) are all domestic only.

[452] FATF, Vulnerabilities of Casinos and Gaming Sector, 2009

[453] Gambling Commission, *Money laundering and terrorist financing risk within the British gambling industry*, 2017

[454] Gambling Commission, *Money laundering and terrorist financing risk within the British gambling industry*, 2017

[455] Note that private lottery operators are possible by Luxembourg law, but none are currently present

[456] "Loi du 22 mai 2009 relative à l'Œuvre de Secours Grande-Duchesse Charlotte et à la Loterie Nationale, with Article 2 stating that *"L'Œuvre a pour missions : […] d'organiser et de gérer la Loterie Nationale.*"

[457] €46 million gross gaming revenue (GGR) per year, with total sales averaging €100 million per year

[458] ~2% of revenues through horse betting and ~2% of revenues through sports betting. Horse betting is organised by LN, conducted via the French PMU, on PMU terminals. Sports betting is conducted via the German ODDSET Group and the German Lotto- und Totoblock, formed by the 16 German State-lotteries. Although sports/horse betting present a higher vulnerability to ML, it represents a very small part of total revenues

[459] World Lottery Association, *"The WLA World Lottery Data Compendium",* 2015

The National Lottery uses **intermediaries** ("points of sale") to sell its products, including supermarkets, petrol stations, newsagents, bars and others, which totalled ~425 in 2019. Its only direct sales channel is online at the National Lottery website, which represents only ~6% of revenues. Around 94% of revenues are generated from tickets sold via points of sales (supermarkets and kiosks with ~60% of sales, petrol stations with ~15% of sales, and the remaining in bars and restaurants). As such, although intermediaries are involved in selling National Lottery tickets, they are not likely to significantly increase ML/TF risk as the products themselves are inherently low-risk.

6.2.4.3. Ad hoc lotteries

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

The low ML/TF risk is driven by the **small volumes involved in the sub-sector**, thus inhibiting large-scale ML/TF activities. Most lotteries are organized at the local level and approved by one of the 102 municipalities, if they are expected to generate less than €12 500. No aggregate data on local ad-hoc lotteries across municipalities is collected, but overall they are unlikely to generate significant proceeds given the low threshold in place. Assuming conservatively that each municipality authorizes three ad hoc lotteries a year for average revenues of €6 000, total revenues generated by local ad hoc lotteries would reach only €2 million per year.

Above the expected revenue level of €12 500, lotteries must be approved by the Minister of Justice. An average of 5-10 lotteries are authorized each year at the national level. Overall, the amounts involved for these national ad hoc lotteries are likely to be limited: They each generate on average between €40 000 and €50 000, leading to an expected annual total of ~€350 000 amongst all of them. Furthermore, authorisations granted by the Minister of Justice provide that 40% of the generated revenue is distributed as wins to the participants.

The ML/TF risk is also reduced by the **low-risk nature of ad hoc lottery organisers.** Until now, all authorisations for lotteries at the national level have been granted to well-known non-profit organisations (such as charities, sports clubs) established in Luxembourg for decades, as for example the Red Cross.

6.2.4.4. Sports betting and online gambling

The level of ML/TF risk from sports betting and online gambling is considered as low in Luxembourg given that no authorised company operates in sports betting or online gambling (except the National Lottery, see above). While **horse/sports betting** activities providers may be authorised under the 1977 Gambling Law, the National Lottery currently has a monopoly on horse/sports betting and only offers offline horse/sports betting, with tickets sold via ~30 retailers for horse betting and ~25 for sports betting with an approximate average yearly revenue of €2 million.

6.2.5. Real estate

The real estate and associated construction sectors are typically regarded as high risk globally. They often involve large monetary transactions and offer the ability to conceal the true source of the funds either directly through physical persons or via layering of the transaction involving multiple legal entities. Indeed, products offered are particularly suited to laundering since they include physical assets such as land and houses which enable storage of monetary value and potential to reap returns (via investment in funds/physical assets). The large number of customers (many of whom will have legitimate activities) could offer a level of anonymity to criminals (who could for instance use physical persons as third parties to obscure the ultimate beneficiary).

Globally, various money laundering real estate techniques have been used for misused for criminals. For example, criminals have purchased a property with cash from criminal proceeds, or used off-shore companies to conceal beneficial ownership. Another popular technique observed globally is financing a property purchase through loan back, meaning the criminals borrow their own criminal money[460].Other commonly used fraudulent techniques include mortgage schemes, manipulation of property price (over/under-valuation, successive sales and purchases), investments schemes, financial entities (criminals purchase real estate through investment funds), complex loans and credit finance.

In Luxembourg, the risk is in line with the global risk rating. The ML/TF is driven by the **large sector size and fragmentation**. The real estate activities sector contributes 8.1 % to the country's gross value added in 2019 with ~€ 4.1 billion[461]. Furthermore, the real estate and construction sector is very fragmented with more than 6 500 enterprises involved in real estate related and construction activities[462] and more than 50 000 employees[463]. Combined production value exceeded €14 billion in 2019.

The vulnerability is amplified as laundering via real estate activities is dependent on the presence and expertise of service professionals, who form a very sophisticated and mature industry in Luxembourg.

Real estate agents, who act as intermediaries in real estate transactions, are particularly exposed to ML/TF, especially given their central role in transaction facilitation.[464] For example, criminals may misuse agents in a deliberate way to disguise the identity of the beneficial owner. Further, agents may be misused to manipulate the market value of a property and allow a criminal to launder illicit money.

In Luxembourg, this sector is **sizeable and fragmented**, driving significant ML/TF risks, with 2 329 real estate agents. The five largest companies account for only ~20% of the total revenue.[465] The combined turnover of real estate agents in 2018 was ~€2.6 billion. Approximately a half of real estate agents have annual turnover less than €120 000, approximately a third have an annual turnover between €120 000 and €620 000, and approximately 15% have annual turnover above €620 000. There is also a **high volume of and value of transactions**, which may drive the ML/TF risk of the sub-sector. In addition, real estate agents have a small proportion of non-resident clients (3-4%), with **geographical risks** adding another layer of opacity to the source of money.

Real estate developers *("promoteurs")* share similar ML/TF risk exposure to real estate agents. They realise the construction programs of properties, and similar to agents, can be involved in operations concerning the purchase or sale of real estate. As such, they may also act as intermediaries in the sub-sector. Similar to agents, real estate developers are a **large and fragmented sub-sector**. They also handle multiple a **large volume and value transactions**. The overall produced volume by the construction sector in Luxembourg in 2019 was ~€8.6 billion. They are introduced in the AML/CFT scope by the 2020 AML/CFT Law.

6.2.6. Dealers in goods

Dealers in goods are exposed to ML/TF given that they offer products of high value that can be easily stored, transported and exchanged at a similar value due to the commoditisation of luxury products. Also, the anonymity offered to clients (via intermediaries) and the high level of secrecy in the industry reinforces the sector's vulnerability. Globally, there have been cases where criminals used to purchase

[460] OECD, *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*, 2019
[461] STATEC, *E2103, Section 7, Code L*
[462] STATEC, latest data available for 2017
[463] STATEC
[464] FATF, Money Laundering and Terrorist Financing Through the Real estate sector, 2007
[465] AED

high value goods in cash and obtained a refund in an alternative money transfer service, legitimising their criminal proceeds[466].

In Luxembourg, dealers in goods are defined in the AML/CFT regulation as entities dealing goods and accepting cash equivalent to €10 000 or more in any currency. These include dealers in precious metals, watchmakers and jewellers, car dealers, art/antiques dealers and luxury goods retailers (e.g. *"maroquinerie"*).

The vulnerability to ML/TF for each of the sub-sectors except car dealers in Luxembourg is limited as they are a **very concentrated**. For instance, although it has ~€4 billion in revenues and 8 000 employees, subsectors are highly concentrated. Only car dealers are moderately fragmented with over 762 dealers as of March 2020[467].

Dealers in precious metals, art and luxury goods have similar attributes including high concentration and considerable cash usage, which drives similar levels of vulnerability. The vulnerability of **dealers in precious metal, jeweller, watchmakers** is linked to the commoditized nature of high-value products but is mitigated by the small size of the sector in Luxembourg. As of 2019, there are 153 entities in this sub-sector. Similarly **art and antique** dealers represent a relatively small industry. Finally, **luxury-good dealers** (e.g. *"maroquinerie"*) are a highly concentrated sector with established companies, which limits inherent risk.

The most vulnerable sub-sector within dealers of objects is **car dealers**. It is a **large** and **fragmented** sector with an estimated 762 entities[468]. In addition, activities such restoration of antique or second-hand cars sale where it is difficult to objectively value the good/service could be used to launder money.

6.2.7. Freeport operators

FATF defines Free Trade Zones as "designated areas within jurisdictions in which incentives are offered to support the development of exports, foreign direct investment (FDI), and local employment"[469]. In recent years, freeports have often been used for long-term storage because of the highly secure environments provided.

Globally, freeports are typically regarded as presenting high ML/TF risks[470]. Freeports have been among the beneficiaries as undeclared money has fled offshore bank accounts as a result of tax-evasion crackdowns in America and Europe. Freeports in other jurisdictions provide high security and confidentiality to their clients, and may not have full information on the ultimate beneficial ownership[471]. They may prove the ability for owners to hide behind nominees, and an array of tax advantages, that further conceal owner identities. Freeports can store high value goods (e.g. works of art), which may be used as a replacement for intra-banks transactions (for instance art works used as warranty and/or payment for drugs shipments). In addition, integration of illegal proceeds can occur through trades in free trade zone, by falsifying the value/quantity of a shipment to justify value transfer.

The Freeport in Luxembourg is located in Luxembourg Findel airport and encompasses 22 000m² of building structure. It is specifically designed for storage of high value goods (such as artwork, vintage cars and fine wines). Humidity, temperature and other storage conditions are adapted. It has direct

[466] Jersey FSC, *AML/CFT Handbook for Estate Agents and High Value Dealers*, 2015
[467] AED
[468] STATEC
[469] FATF, *Money Laundering vulnerabilities of Free Trade Zones,* March 2010
[470] FATF, *Money Laundering vulnerabilities of Free Trade Zones*, March 2010
[471] European Parliamentary Research Service, *Money laundering and tax evasion risks in free ports*, October 2018

tarmac access on the cargo runway to reduce as much as possible package manipulations. Its fire system is designed to protect artwork (vacuuming oxygen in the rooms). Strong rooms are up to 300m² in surface. Gold is allowed, but cash is not. It is managed by the Freeport Management Company SA. Four licensed freeport operators rent space at the Freeport as of March 2020. One operator works mainly for galleries and museum, one for art intermediaries, one specialises on gold storage and the fourth one for banks (e.g. gold), which results in second-order ML/TF exposure.

In Luxembourg, the ML/TF risk lies primarily with the freeport operators as they interact directly with clients and handle the goods. In line with global risk assessments, the ML/TF vulnerability is primarily driven with their **high-risk nature of activities**, as they allow storage for different types of high-value goods. In addition, the freeport have large **international flows**, which may expose them to ML activities from other countries.

However, in Luxembourg a comprehensive package of legislative and operational measures has ensured transparency and the application of AML mitigating measures. Since 2015, freeport operators in Luxembourg are required to identify the beneficial owners of the goods that were brought in by their clients. Galleries, merchants and dealers are often unable to share this information on their clients, as a major share of their clients prefer privacy. Clients cannot use offshore companies, trusts, lawyers, nominees or galleries to shield their ownership of goods in the Luxembourg Freeport. Those clients may prefer using other freeports where information on ultimate beneficial ownership is not required[472]. Therefore, compared to similar structures internationally, the Freeport in Luxembourg may less be attractive for criminals for ML purposes, and as such be much less likely to be abused for ML/TF purposes.

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

6.3. Legal entities and arrangements

Legal entities and arrangements are commonly regarded to be highly vulnerable to ML/TF crimes. As the OECD observes, "almost every economic crime involves the misuse of corporate vehicles"[473] since they might help conceal origin of funds and/or allow funds to be moved overseas. This is because movements of large amounts of proceeds between legal entities and arrangements may attract less attention and suspicion than movements between individuals. Also, legal entities and arrangements can help conceal identity of ultimate beneficial owners and make the link to criminality more difficult to establish by using layers of entities in multiple jurisdictions.

As a result, the number of cases involving co-mingling of illegitimate and business activities has increased worldwide[474]. Although only a small minority of corporate vehicles are used for money laundering, the amounts at stake are estimated to be very large. In 2011, out of the 213 grand corruption cases reviewed by World Bank, 150 involve corporate vehicles with a total of $56.4 billion involved in those cases[475].

The following two case studies illustrate the misuse of LE&A as a means to launder assets.

Case Study 17: Concealment of assets in Dutch and Luxembourgish companies through complex corporate operations and multiple trusts[476]

In 2009, the *Nucleo Polizia* of Milan conducted a preventive seizure of funds, for a total value of €1.3 billion, held in the Channel Islands and traceable to a single family. The assets were concealed through a complex network of trust accounts, hiding the beneficiaries of assets (public debt securities and cash). The investigation established that over a 10-year period, between 1996 and 2006, the subjects placed their assets in Dutch and Luxembourgish companies through complex corporate operations, and by transferring the assets to different trusts in the Channel Islands. In December 2009, the funds were legally repatriated through a tax amnesty. Moreover, the investigation identified chartered accountants who had facilitated the concealing of funds over times, through multiple trusts, with the aim of facilitating laundering and reinvestment.

This case brings to light two key elements, which, in conjunction, may constitute indicators of misuse of legal entities and arrangements:

- A legal person or arrangement incorporated in a low-tax jurisdiction or international trade or financial centre;
- Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense.

Case Study 18: Tax fraud involving a Luxembourg numbered account in the name of a foundation

A doctor (the suspect) received payments from the pharmaceutical industry with which he was in business, in amounts that varied per contract. These payments, which can be considered income, were not paid into one of the suspect's Dutch bank accounts, but into Luxembourg numbered

[473] See for instance, OECD, *Behind the corporate veil: using corporate entities for illicit purposes,* 2001

[474] World Economic Forum, *Organised Crime Enablers, Global Agenda Council on Organized Crime*, July 2012

[475] World Bank, *The Puppet Masters: How the corrupt use legal structures to hide stolen assets and what to do about it*, October 2011

[476] See FATF Egmont Group Report on Concealement of Beneficial Ownership (2018) for more detail

accounts, and in the name of a foundation. The suspect never declared the balances of these Luxembourg bank accounts in his income tax returns.

This case brings to light several key elements, which, in conjunction, may constitute indicators of misuse of legal entities and arrangements:

- Multiple bank accounts without good reason, and/or bank accounts in multiple international jurisdictions without good reason;
- Transaction involving a numbered account;
- Focus on aggressive tax minimisation strategies;
- Correct documents not filed with the tax authority;
- Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client.

Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre.

Table 20: Legal entities and arrangements. Inherent risk assessment (at subsector-level)

Sector	Inherent risk	Sub-sectors	Inherent risk
Legal entities and arrangements	**High**	*Sociétés commerciales**	**Very High**
		Domestic "fiducies"*	**Very High**
		Foreign trusts	**Very High**
		Associations sans but lucratif (ASBL) and *fondations* with Non-governmental organisations (NGO) status	**High**
		Sociétés civiles	**Medium**
		Other *associations sans but lucratif (ASBL)*	**Medium**
		Other *fondations*	**Low**
		Other legal entities	**Low**

**Note that many of these corporations may already be entities supervised by AML/CFT competent authorities depending on their industry sector (e.g. financial corporations by CSSF and CAA). Additionally, most of fiducies are expected to be managed under fiduciary agents, which in Luxembourg are required to be AML/CFT supervised entities, if the fiducie is to be awarded legal protection under the Fiducies and Trusts 2003 Law (see section on Legal arrangements). However, at present available data does not allow for a granular quantification of the number of legal entities or arrangements per a given industry and with its fiduciary agent under a given AML/CFT supervisor.*

6.3.1. Legal entities

Legal entities are legal persons who are recognised legal capacity. A legal entity has legal capacity to enter into agreements or contracts, assume obligations, incur and pay debts, sue and be sued in its own right, and to be held responsible for its actions. In Luxembourg, legal entities include five main types as per the table below. All legal entities incorporated in Luxembourg must be registered with the *Registre de Commerce et des Sociétés* ("RCS") as per 2002 RCS Law. The RCS counts 137 444 legal entities [477] in the registry as of June 2020. Basic information available in the registry slightly differs by type of company (e.g. SAs provide less information on ownership than SARLs due to their nature).

The RCS, as of 2019, is managed by the LBR (Luxembourg Business Registers). The LBR is an economic grouping placed under the authority of the Minister of Justice, which consolidates the State, the

[477] Data request to LBR, March 2020

Chamber of Commerce and the Chamber of Trades. The LBR's mission is to manage and to develop, beyond the RCS, the different registers it is trusted with, each with its own legal framework.

Table 21: Legal entity taxonomy in Luxembourg

Legal entity types, as registered in the RCS	Mapping to Luxembourg legal framework
Sociétés commerciales	• As per article 100-2 of the 1915 Companies Law: • SNC (Société en nom collectif) • SCS (Société en commandite simple) and Société en commandite spéciale[478] • SA (Société anonyme) and SAS (Société par actions simplifiée), including SOCOOP (Société cooperative organisée comme une SA) • SCA (Société en commandite par actions) • SARL (Société à responsabilité limitée) and SARLS (Société à responsabilité limitée simplifiée) • SC (Société cooperative) • SE (Société Européenne)
Sociétés civiles	• As per article 1832 of the Civil code
Association sans but lucratif (non-profit organisations, including NGOs)	• Non-profit organisations, as per 1928 NPOs Law
Fondations	• Foundations, according to the 1928 NPOs Law
Other legal entities	• All other legal entities registered with RCS, including, but not limited to: • Groupements d'intérêt économique • Groupements européens d'intérêt économique • Associations agricoles • Etablissements publics

An overview of the existing legal entities as of June 2020 registered with the *Registre de Commerce et des Sociétés* is provided below.

Table 22: Breakdown of existing legal entities as registered in the RCS, 2017-2020

Type	2017		2018		June 2020	
	Number	% total	Number	% total	Number	% total
Sociétés commerciales, incl.	**124 729**	**87%**	**129 128**	**86%**	**120 270**	**88%**
Société à responsabilité limitée[479]	71 347	-	75 321	-	74 960	-
Société anonyme[480]	48 048	-	47 311	-	37 402	-
Société en commandite[481]	3 058	-	4 104	-	5 634	-
Société en commandite par actions	1 675	-	1 800	-	1 937	-
Société en nom collectif	423	-	413	-	174	-
Société cooperative	146	-	150	-	129	-
Société Européenne	32	-	29	-	34	-
Associations sans but lucratif (incl. NGOs)	**10 838**	**8%**	**11 246**	**7%**	**8 318**	**6%**

[478] While *Sociétés en commandite spéciale* are not recognised as a legal person separate from its members by article 100-2 of the 1915 Companies Law, seeing as the LBR registers them as corporations, they are included in our count

[479] Includes Société à responsabilité limitée simplifiée

[480] Includes *Société coopérative organisée comme une SA,* and *Société par actions* simplifiée

[481] Includes *Société en commandite simple* and *Société en commandite spéciale*

Sociétés civiles	**4 782**	**3%**	**4 998**	**3%**	**5 486**	**4%**
Fondations (includes NGOs, where applicable)	**211**	**0%**	**214**	**0%**	**217**	**0%**
Other legal entity types	**3 278**	**2%**	**4 581**	**3%**	**3 153**	**2%**
Total registered in RCS	***143 838***	***100%***	***149 997***	***100%***	***137 444***	***100%***

Source: *Registre de Commerce et des Sociétés. Note, numbers for 2017 and 2018 may differ from the 2018 NRA. We have revised them for consistency with the 2020 classification*

The national vulnerability derives from a high number of corporations and special legal entities: 137 444 legal entities as of June 2020, with a high perceived level of foreign ownership and international operations and businesses. It is also noted that in addition, ~25 000 legal entities are under judicial or voluntary liquidation, or under insolvency proceedings under judicial control and are thus perceived to have a lower ML/TF risk (given that they are being managed by insolvency practitioners or lawyers).

The table below summarises the sectoral split per legal entity types, described above.

Table 23: Sectoral split of legal entities as of 30.06.2020 (registered with RCS)

Sector	*Sociétés commerciales*	*ASBL*	*Sociétés civiles*	*Fondations*	Other legal entities
Agriculture, forestry and fishing	176	1	103	-	14
Mining and quarrying	14	-	-	-	-
Manufacturing	991	-	2	-	3
Electricity, Gas, Steam and Air Conditioning supply	147	1	121	-	9
Water supply	61	1	-	-	1
Construction	6 551	-	37	-	5
Wholesale and retail trade	10 974	1	7	-	13
Transportation and storage	1 849	2	4	-	3
Accommodation and food service activities	4 029	8	6	-	1
Information and communication	3 366	47	1	1	13
Financial and insurance activities	65 690	6	278	1	1 507
Real estate activities	5 916	2	2 996	2	8
Professional, scientific and technical activities	8 800	59	74	4	37
Administrative and support service activities	3 542	47	428	-	14
Public administration and defence	1	52	-	-	32
Education	395	111	2	11	10
Human health and social work activities	434	330	15	34	38
Arts, entertainment and recreation	411	1 416	41	7	16
Other service activities	1 222	3 025	1	82	22
Activities of extraterritorial organisations and bodies	-	1	-	-	-
Unknown NACE	6 001	3 208	1 370	75	1 417
Total	***120 270***	***8 318***	***5 486***	***217***	***3 153***

Sociétés commerciales (corporations) are the main type of legal entities in Luxembourg, totalling 120 270 in June 2020. They are registered at the RCS, which is run by the LBR.

As per article 100-2 of the 1915 Companies Law, supplemented by the Law of 12 July 2013, and the EC Regulation 2157/2001 (Art. 16.1), the law recognises seven types of legal entities:

- SNC *(Société en nom collectif)* – general corporate partnership/unlimited company
- SCS *(Société en commandite simple)* – common limited partnership
- SA (*Société anonyme*), by the Law of 10 August 2016, and the SAS (Société par actions simplifiée) – public company limited by shares and simplified joint stock company
- SCA (*Société en commandite par actions*) – corporate partnership limited by shares
- SARL (*Société à responsabilité limitée*) and SARLS (*Société à responsabilité limitée simplifiée*) – private limited liability company, and simplified private limited liability company
- SC (*Société cooperative*) – co-operative society
- SE (*Société Européenne*) – European company

Each of the above constitutes a legal person separate from its members.

Temporary commercial companies (*Sociétés commerciales momentanées*), commercial companies by participation (*Sociétés commerciales en participation*), and special limited partnerships (*Sociétés en commandite spéciale*), do not have a legal personality distinct from that of their members. However, as the LBR registers *Sociétés en commandite spéciale,* we have included them in our count.

Out of 137 444 legal entities registered, the RCS counted 71 981 SARL and 37 135 SA in June 2020: 59 099 of the registered entities were financial services entities, excluding insurance and pension funding – the largest segment; 5 689 entities were real estate companies.

Although these entities are widespread and play an important and legitimate role in many of the sectors in Luxembourg's economy, they may also be exploited to conduct ML/TF. According to international research, entities can be structured to make beneficial ownership more opaque, and can be used to disguise and convert illicit proceeds. Luxembourg has immobilised bearer shares pursuant to a legislation in force since 2014[482]. All existing and new bearer shares must be deposited with a professional submitted to AML/CFT requirements. Shares that have not been registered by February 2016 had been cancelled and their value deposited with the Treasury's *Caisse de consignation*.

Sociétés civiles are a flexible company structure (e.g. no capital required) traditionally used by Luxembourgish residents to manage non-commercial real estate assets in a tax transparent manner, per article 1832 of the Civil Code[483]. There have been no known cases of ML/TF through *sociétés civiles*. Although far less than commercial companies in number, their number is still relatively high (5 486[484] as of June 2020) and they have no obligation to submit annual accounts or to audit accounts, which further exposes *Sociétés civiles* to ML/TF. This type of company structure is mostly used for real estate management in the form of a *Société civile immobilière*. It can also concern civil, agricultural, liberal or intellectual professions. *Sociétés civiles* are registered at the RCS.

ASBLs "*associations sans but lucratif***"** (non-profit organisations, or NPOs) operating locally without exposure to high risk jurisdictions are more fragmented (8 318 entities as of June 2020[485]). Even though no centralised taxonomy exists to classify them (e.g. by type of activity), most of them are

[482] Law of 28 juillet 2014 relative à l'immobilisation des parts au porteur.

[483] "Une société peut être constituée par deux ou plusieurs personnes qui accepte de mettre en commun quelque chose choisit en vue de partager le bénéfice qui pourra être résulter ou, dans les cas prévus par la loi, par acte de volonté d'une personne bine qui affecte l'exercice d'une activité déterminée.", Article 1832 du code civil

[484] Data request to LBR, June 2020

[485] Data request to LBR, August 2020

thought to be local sports clubs and community associations, with a limited number of non-Luxembourg resident members. Many are assembled in broader national federations (e.g. *Fédération nationale de football*) allowing to determine their type of activity. All ASBLs are registered at the RCS. According to the 1928 NPO law, all ASBLs have a legal requirement to yearly file with the RCS the list of their members (article 3) as well as any change in the composition of the board of directors (article 10). ASBLs do not need to submit financial statements unless they accept donations or wills, receive public funds, or are recognised as being of public interest by Grand-Ducal decree, in which case they are treated (and have similar obligations) as *Fondations*. All donations made to ASBLs are irrevocable.

In view of their activities (mostly sportive and cultural, with no fund raising for charitable purposes) and ownership structure, most ASBLs are estimated to have a low exposure to ML/TF threats; but given their relatively high number, the inherent risk is evaluated as medium for the local ASBL sector as a whole until a national assessment of their activities will permit a more granular assessment, in line with a conservative approach.

Notwithstanding, **NGOs** (non-governmental organisations) have been flagged by FATF as being exposed to the risk to be abused for terrorism financing. This covers essentially NPOs that operate in high-risk jurisdictions (including areas of conflict with an active terrorist threat). It should be noted NPOs with a goal of international cooperation and development (NGOs for Development) are specifically defined[486] and accredited by the Ministry of Foreign Affairs, *Ministère des Affaires étrangères et européennes*, (MAEE); around 100 of such NGOs were in existence as of year-end 2019[487]. These NGOs for Development mostly take the legal form of an ASBL. In some instances, foundations, when pursuing development projects in addition to their national public utility purpose, might be recognized as NGOs for their international activity. Given MAEE finances NGOs, it performs checks on NGOS and their projects to ensure appropriate use of government funds. When receiving public subsidies, NGOs must have their accounts audited and submitted to the RCS annually. The number of NPOs with a potential exposure to TF is however still low.

Any person may, subject to approval by grand-ducal decree, allocate by authentic act or by will all or part of his or her assets to the creation of a ***foundation***, which has civil personality under the conditions set out below. Only foundations that essentially with the help of the income from the capital assigned to their creation or collected and excluding the pursuit of material gain and are intended to carry out a work of a philanthropic, social, religious, scientific, artistic, educational, sporting or tourist nature are considered to be foundations (217 foundations are registered in the RCS as of 30 June 2020[488]). Any authentic declaration and any testamentary disposition made by the founder with a view to creating a foundation shall be communicated to the MoJ for approval. Until it is approved, the founder may withdraw his or her declaration. This right does not belong to the executor or to the heirs and successors.

In Luxembourg, foundations are less vulnerable to ML/TF; the number of entities is relatively limited (217 entities as of June 2020[489]) and no private foundations are allowed – all entities act purely in the public interest and donations (including initial founding) made are irrevocable. They have a low number of non-Luxembourg resident Board members, have mandatory submissions of their accounts to the Ministry of Justice on an annual basis, and must be registered with the RCS (article 34). Still, foundations typically involve large sums of money which may make identification of suspicious activity and criminal intent difficult to detect, and hence may still be somehow exposed to ML/TF risk.

Other legal entities are less vulnerable to ML/TF due to their limited number, regulation and ownership structure, such as "*Groupements d'intérêt économique* (GIE)" (82 in June 2020),

[486] Article 7 of *loi du 9 mai 2012 modifiant la loi modifiée du 6 janvier 1996 sur la coopération au développement*

[487] As per Ministry's (MAEE) website: https://cooperation.gouvernement.lu/fr/partenaires/ong-partenaires.html

[488] Data request to LBR, August 2020

[489] Data request to LBR, August 2020

"*Groupements européens d'intérêt économique* (GEIE)" (58 as of June 2020), "*Associations agricoles*" (113 as of June 2020), "*Etablissements publics*" (117 as of June 2020).

6.3.2. Legal arrangements

Legal arrangements in Luxembourg are defined and recognised in the 2003 Fiducies and Trusts Law[490]. These comprise domestic legal arrangements ("fiducies") and foreign Trusts.

Domestic "*fiducies*" were established in 1983 through a Grand Ducal Decree. According to article 5 of the 2003 Fiducies and Trusts Law, a fiduciary contract is an agreement whereby the settlor (or *fiduciant*) agrees with the fiduciary (or *fiduciaire*) that the latter will become the owner of certain fiduciary assets (the fiduciary estate or *patrimoine fiduciaire*) under agreed conditions. These conditions include the fiduciary mission (instructions for the fiduciary over managing the entrusted assets) and the obligation to clearly separate each fiduciary estate (entrusted assets of each agreement) from other property belonging to the fiduciary agent or other fiduciary estates entrusted to him. The transfer of ownership over assets and the requirement of two parties for each agreement (rather than by unilateral action) distinguishes domestic fiducies in Luxembourg from the Anglo-saxon trust structure.

Luxembourg law recognises **foreign trusts** and does not prohibit a resident from acting as trustee, administrator or manager or from having the responsibility to distribute profits or to administer a trust that is constituted under foreign legislation.

- Tax purpose:

  Luxembourg law requires the registration with the AED of contracts subscribed by fiducies concerning real estate, aircraft, ships or boats registered in Luxembourg.

  Luxembourg taxation rules provide that income from Luxembourg sources received via a fiducie is taxable in the hands of the settlor. The resulting tax obligations depend on the nature of the settlor (natural or legal person). Paragraph 164 of the general tax law provides that where a taxpayer claims to derive income as a fiduciary agent or representative, he has to demonstrate for whose benefit he acts. If this is not the case the income is allocated to the fiduciary agent. The tax law also provides that any person holding an asset in the capacity of fiduciary must be able, upon demand, to identify the real owner of the property, and this implies the availability of such information. The Luxembourg authorities point out that in practice, the use of fiducies in Luxembourg is rather limited. In any case, the fiduciary must be able to identify the settlor to the tax authorities.

  The activity of professional trustee is mainly exercised by financial institutions.

- AML/CFT purpose:

  The AML/CFT Law defines the beneficial owners of the Luxembourg fiducies and foreign trusts in compliance with the standard as the following:

  (i) the "settlor(s)";
  (ii) the "fiduciaire(s)" or "trustee(s)";
  (iii) the "protector(s)", if any;
  (iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

[490] Loi du 27 juillet 2003 - portant approbation de la Convention de La Haye du 1er juillet 1985 relative à la loi applicable au trust et à sa reconnaissance; - portant nouvelle réglementation des contrats fiduciaires, et - modifiant la loi du 25 septembre 1905 sur la transcription des droits réels immobiliers

(v) any other natural person exercising ultimate control over the fiducie or trust by means of direct or indirect ownership or by other means.

In line with the 4AMLD, a consolidated database of BO of fiducies and trusts has been set up by the Law of 10 July, 2020.

6.4. Cross cutting vulnerabilities

6.4.1. Trust & corporate service providers (TCSPs)

As intermediaries providing a key link between institutions and their customers, Trust and corporate service providers (TCSPs) play an important role in the global economy. TCSPs provide often assistance to their clients in the setup, management, and administration of their affairs, and can thereby significantly impact transactional flows through the financial systems[491] and prevent the misuse of legal persons and arrangements for ML/TF purposes.

Several international and national organisations have highlighted the exposure of TCSPs to ML/TF, and the importance of professionals taking appropriate AML/CFT measures. For example, FATF has identified the TCSP sector as particularly exposed to ML/TF and has published several reports to assist firms and supervisors in mitigating the risks associated with their activities. Most recently, these reports have included the 2019 "*Guidance for a risk-based approach, TCSP sector*"[492] describing what a risk-based approach for both professionals and supervisors would entail and detailing specific guidance for TCSPs and elements of a robust supervisory approach.

FATF defines TCSPs as professionals providing any of the below services to third parties[493]:

- Acting as a formation agent of legal persons;
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- Providing a registered office, business address or accommodation correspondence or administrative address for a company, a partnership or any other legal persons or arrangements;
- Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; and
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

6.4.1.1. Vulnerability of TCSPs

TCSPs are often involved in the establishment and administration of legal persons and arrangements, in many cases playing a key role as gatekeepers. However, they are sometimes misused or abused by criminals for ML/TF purposes due to the central role that they play in the economy and investments and given the nature of the services they provide. For instance, in Luxembourg, they may be involved in changes to the shareholding or structure of legal entities, they can provide advice to structure some transactions, etc.

Criminals can abuse or misuse TCSPs for different reasons, including concealing ultimate beneficial ownership of funds and legitimising the integration or layering of criminal proceeds within the financial system, through various forms of investments and legal structures. The complexity of structures reduces the ability of investigators to trace the origin and ownership of assets held. This is illustrated in the following two case studies (below).

[491] FATF, *Money Laundering using TCSPs*, 2010

[492] FATF, *Guidance for a risk-based approach, TCSP sector*, 2019

[493] FATF, *Methodology, Glossary*

Case Study 19: Use of nominee director and shareholder services to conceal BO indentity[494]

International Company A headquartered in an EU jurisdiction maid corrupt payments to a government employee using nominee director services and international transactions in the following way:

- International Company B was registered in a foreign jurisdiction, with a government employee as the beneficial owner.
- International Company B used nominee shareholders and directors provided by TCSPs, thereby permitting the concealment of the government employee's identity.
- Payments were made via a European bank account of a subsidiary of International Company A to another of its accounts in Eastern Europe, and via an enterprise registered in Asia. These funds were then paid into bank accounts in a foreign jurisdiction.
- The funds were transferred from the bank accounts in foreign jurisdiction to a Luxembourg bank account of International Company B, to which the government employee had access (being the BO).

Case Study 20: Abuse or misuse of set-up services and complex legal structures for the creation of company networks for ML purposes[495]

A law enforcement operation identified an accountant, J, who was believed to be part of the criminal organisation involved in money laundering and re-investment of illicit proceeds derived from drugs trafficking led by X.

J's role was mainly that of a "legal and financial consultant". His task was to analyse the technical and legal aspects of the investments planned by the organisation and identify the most appropriate financial techniques to make these investments appear legitimate from a fiscal stance. He was also to try, as much as possible, to make these investments profitable. J was an expert in banking procedures and most sophisticated international financial instruments. He was the actual financial "mind" of the network involved in the re-investment of proceeds available to X. J operated by sub-dividing the financial transactions among different geographical areas through triangle transactions among companies and foreign credit institutions, by electronic transfers and stand-by credit letters as a warrant for commercial contracts, which were later invested in other commercial activities.

[494] Case study presented FATF and Egmont Group, *Report on Concealment of Beneficial Ownership*, 2018

[495] Source: extracted from website of JE Financial Services Commission

6.4.1.2. Luxembourg's TCSP landscape

Definition of TCSPs

The 2004 AML/CFT Law defines trust & corporate service providers (*"prestataires de services aux sociétés et fiducies")* as any natural or legal persons who provide, in a professional capacity, any of five trust and corporate services to third parties. That is, TCSPs are defined by the activities they perform, rather than there being a specific license for TCSPs.

The definition of a "*prestataires de services aux sociétés et fiducies"* in the 2004 AML/CFT law is in line with FATF's definition of TCSPs, which defines TCSPs as any natural or legal persons that are not covered elsewhere under the FATF Recommendations, and which as a business provide any of five TCSP services to third parties.

The table below maps the five TCSP services as described in the 2004 AML/CFT Law to the description of the respective service as per the FATF definition described in FATF's "Guidance for a Risk-Based Approach for Trust & Company Service Providers (TSCPs)".

Table 24: Mapping of TCSP services described in the 2004 AML/CFT Law, to FATF guidance on TCSPs

	TCSP services described in 2004 AML/CFT Law[496]	Mapping to FATF definition[497]
a)	Forming companies or other legal persons	**Incorporation:** Acting as a formation agent of legal persons
b)	Acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons	**Directorship and secretarial services:** Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
c)	Providing a registered office, business address, correspondence or administrative address "or business premises" and other related services for a company, a partnership or any other legal person or arrangement	**Domiciliation:** Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement
d)	Acting as, or arranging for another person to act as, a *fiduciaire* in a *fiducie*, a trustee of an express trust or an equivalent function in a similar legal arrangement	***Fiducie/*trust**: Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement
e)	Acting as, or arranging for another person to act as, a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in accordance with European Union law or subject to equivalent international standards	**Nominee shareholder:** Acting as (or arranging for another person to act as) a nominee shareholder for another person

[496] Article 1-8 of the 2004 AML/CFT law as amended in March 2020

[497] FATF (2019), Guidance for a Risk-Based Approach for Trust & Company Service Providers (TSCPs), FATF, Paris, www.fatf-gafi.org/publications/documents/rba-trust-company-service-providers.html

Professionals authorised to do TCSP activities

A range of professions in Luxembourg conducts at least one (or more) of what the 2004 AML/CFT Law defines as TCSP activities as described above. Entities that act as TCSPs include banks, investment firms, specialised PFSs, professionals of the insurance sector (PSA), lawyers, audit professionals[498] and chartered professional accountants[499], amongst others. However, only the activity of domiciliation is regulated by the 1999 Domiciliation Law and restricted to credit institutions, PFSs, PSAs, lawyers, auditors and chartered accountants. TCSPs are thus a broad and diverse category in Luxembourg, given the range of professionals that are legally authorised to conduct such activities.

The table below describes the professions authorised to carry out TCSP activities in Luxembourg, the relevant laws that underpin them and their respective AML/CFT supervisor.

Table 25: Professionals authorised to carry out any TCSP activities in Luxembourg[500]

AML/CFT supervisor	Professionals authorised to carry out TCSP activities	Relevant laws
CSSF	Banks and credit institutions	1993 "LSF Law"[501], Part I, Chapter 1
	Investment firms	1993 "LSF Law", Part I, Chapter 2, Section 2, Subsection 1
	Management companies	2010 "OPC Law"[502] and 2013 "AIF Law"[503]
	Three types of specialised PFSs[504], including with the following licenses:	
	• Family Offices	1993 "LSF Law", Article 28-6
	• Corporate domiciliation agents	1993 "LSF Law", Article 28-9
	• Professionals providing company incorporation and management services	1993 "LSF Law", Article 28-10
CAA	Professionals of the insurance sector (PSA)	2015 Insurance Law, Articles 264, 265 and 266[505]
OEC	Chartered professional accountants	1993 "LSF Law", Article 28-9 and 28-10[506] 1999 Chartered Professional Accountants Law 2016 Audit profession Law
IRE	(Approved) statutory auditors and (approved) audit firms	

[498] In this document, the term "audit professionals" covers equally the statutory auditors ("réviseurs d'entreprises"), the approved statutory auditors ("réviseurs d'entreprises agréés"), audit firms ("cabinets de révision") and approved audit firms ("cabinets de révision agréés")

[499] Each profession mentioned in paragraphs 1 to 8 of Article 2(1) of the 2004 AML law

[500] Ministry of Finance, *National Risk Assessment of Money Laundering and Terrorist Financing*, 2018.

[501] **1993 LSF Law**, defining, amongst others, which professionals under the supervision of CSSF can act as TCSPs (i.e. banks; investment firms; family offices; corporate domiciliation agents and professionals providing company incorporation and management services).

[502] **2010 OPC law,** on undertakings for collective investment

[503] **2013 AIF law,** on alternative investment fund managers

[504] Including support professionals of the financial sector providing TCSP services

[505] 2015 Insurance Law: Domiciliation services can be provided by Management companies of captive insurance undertakings and Management companies of reinsurance undertakings – Directorship services can be provided by Management companies of reinsurance undertakings and Management companies of pension funds

[506] Based on the professionals listed in the Law of 31 May 1999 "(Domiciliation Law"), Art. 1(1): "Only a registered member of one of the following regulated professions established in the Grand-Duchy of Luxembourg may act as a domiciliation agent of companies: a credit institution or another professional of the financial sector and the insurance sector, an attorney-at-law ("*avocat à la Cour*") included in list I and a European lawyer practising under his home-title professional title included in list IV referred to in Art. 8(3) of the amended Law of 10 August 1991 on the profession of avocat, *réviseur d'entreprises* (statutory auditor), *réviseur d'entreprises agréé* (approved statutory auditor) or accountant."

AML/CFT supervisor	Professionals authorised to carry out TCSP activities	Relevant laws
OAL/OAD	Lawyers (list I and IV of the Bar[507])	
AED[508]	Other professions offering TCSP services	2004 "AML Law", Art.(2)1 para.13(a)
	• Business centres	
	• Directors	

The nature of the services offered can also differ significantly between different types of professionals. For example, the nature of TCSP services provided by banks has evolved in recent years, and many credit institutions have shifted from providing TCSP services in-house, to creating specific TCSP entities within the group and increasingly sending clients to third-party service providers (e.g. domiciliation agents). Similarly, the nature of domiciliation services performed by asset managers differs from those of specialised PFSs (i.e. the former focusing on the creation of SPVs to separate investments from client assets). Management companies only provide domiciliation services to entities linked to them. They do not provide third-party domiciliation.

In addition, while many professions can offer TCSP activities, not all of them do in practice (and some of them only offer or conduct a subset of activities). For example, even though accountants are legally authorised to conduct four out of the five TCSP activities, not all accountants may do all four, or even one TCSP activity in their day to day job. To put the sector into perspective, the size of these sub-sectors, as provided in previous sections in this NRA, is provided in the table (below). This table (below) provides an overview of the TCSP landscape in Luxembourg, indicating which professions are legally authorised to perform which TCSP activities and the total sector sizes as a whole (without discriminating how many are conducting TCSP activities in practice given absence of aggregate sector data).

[507] Law of 10 August 1991 ("Lawyers Law"): List I lawyers defined as court advocates (*avocat à la Cour)* who are fully qualified Luxembourg lawyers; List IV lawyers defined as EU admitted lawyers (*avocat de l'UE exerçant sous son titre d'orgine)* who are foreign lawyers from the European Union practising under their original professional title

[508] These other professions have business associations – *Association luxembourgeoise des centres d'affaires* (ALCA) and *Institut luxembourgeois des administrateurs* (ILA) – but membership is optional and not self-regulating

Table 26: TCSPs – Overview of professions performing TCSP activities as at 31 December 2019

		TCSP activity typically performed (as defined in 2004 AML/CFT Law)							
Supervisor/ SRB	**Professionals**	Sector size: # of entities[509] (as per NRA vulnerabilities sections)	Sector size: # entities actually offering TCSP activities	Size: Total revenue of all activities performed by relevant entities[510] (as per NRA vulnerabilities sections)	Incorporation	Directorship and secretarial	Domiciliation	*Fiducie*/ trust[511]	Nominee shareholder
CSSF	Banks and credit institutions	128	33	~€23.8 billion	✔	✔	✔	✔	✔
	Investment firms	99	16	~€9 million[512]	✔[513]	✔[514]	✔[515]	✔	[516]
	Management companies	413	100[517]	n.a.			✔[518]		
	Specialised PFSs: Professionals providing company incorporation and management services	107[519]	92[520]	~€0.7 billion[521]	✔	✔		✔[522]	

[509] Where no disctinction can be made between professionals that do and those that do not perform TCSP activities, this number reflects the total number of professionals in the sub-sector; otherwise, it is specified

[510] No distinction can be made between the revenues of professionals that come from TCSP activitities, and the revenues that come from other activities, therefore the revenue number reflects the total revenue of professionals in the sub-sector

[511] Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement

[512] This amount corresponds to the total revenue of the investment firms that provide TCSP activities

[513] An investment firm must hold a "Professionals providing company incorporation and management services" license to provide incorporation services

[514] An investment firm must hold a "Professionals providing company incorporation and management services" license, a "Domiciliation agent" license or a "Family Office" license to provide directorship and secretarial services

[515] An investment firm must hold a "Domiciliation agent" license to provide domiciliation services

[516] No, except CRR Investment Firms (only if agreed for ancillary service 1 of Section C of Annex II of the 1993 LSF Law)

[517] Only for entities which are related to them (e.g. SPV for Private equity funds). No third party domiciliation.

[518] The Management companies only provide domiciliation services to entities linked to them. No third party domiciliation.

[519] CSSF data, 2019

[520] CSSF data, 2019, including the 3 support professionals of the financial sector providing TCSP services

[521] Total revenue of the 3 support PFS providing TCSP services is not included

[522] Specialised PFSs are authorised to provide trust services, but cannot act as *fiducie* under Law of 27 July 2003 on *Fiducies* and Trusts, Art. 4

Supervisor/ SRB	Professionals	Sector size: # of entities[509] (as per NRA vulnerabilities sections)	Sector size: # entities actually offering TCSP activities	Size: Total revenue of all activities performed by relevant entities[510] (as per NRA vulnerabilities sections)	TCSP activity typically performed (as defined in 2004 AML/CFT Law)				
					Incorporation	Directorship and secretarial	Domiciliation	*Fiducie*/ trust[511]	Nominee shareholder
	Specialised PFSs: Corporate domiciliation agents				✓	✓	✓	✓[523]	✓
	Specialised PFSs: Family offices				[524]	✓	[525]	✓[526]	✓
CAA	Professionals of the insurance sector *("Professionnels du Secteur de l'Assurance", or "PSA")*	24	12	€37 million	✓	✓	✓	✓	✓
OEC	Chartered professional accountants ("*Experts-comptables*")	1 170	n.a.	n.a	✓	✓	✓	✓	✓
IRE	Audit firms *("Cabinets de révision (agréées)")*	78	30	n.a.	✓	✓	✓	✓	✓
	Sole Practitioners	24	15	n.a.			✓		
OAL/OAD	Lawyers *("Avocats")*	2 917	729	n.a.	✓	✓	✓	✓[527]	✓
AED	Business centres	76	76	€36 million			✓		
	Directors	722	722	€52 million		✓			

[523] Specialised PFSs are authorised to provide trust services, but cannot act as *fiducie* under Law of 27 July 2003 on *Fiducies* and Trusts, Art. 4

[524] A Family Office must also hold a "Professionals providing company incorporation and management services" to provide incorporation services

[525] A Family Office must also hold a "Domiciliation agent" license to provide domiciliation services

[526] Specialised PFSs are authorised to provide trust services, but cannot act as *fiducie* under Law of 27 July 2003 on *Fiducies* and Trusts, Art. 4

[527] Can assist clients being fiduciaries or managing a fiducie themselves

6.4.1.3. Assessment of the vulnerability of TCSPs in Luxembourg

Overview of TCSP inherent risks

The ML/TF vulnerabilities assessment of the TCSP sector in this section is performed across the different TCSP services as described by the 2004 AML/CFT Law, on aggregate. The assessment is performed across six dimensions, in line with the guidance of FATF on the risk-based approach for TCSPs[528].

Luxembourg TCSPs are particularly exposed to ML/TF, primarily due to four main factors:

- The fragmented landscape of types of professionals acting as TCSPs, all of which are assessed to be vulnerable (given these professions' structure, size and ownership);
  - Includes 13 types of entities, from banks to lawyers
  - These are regulated by nine different supervisors (designated competent authorities or SRBs)
- The exposure of Luxembourg's international financial centre to business originating from multiple jurisdictions;
  - The country's open economy, contributing to significant diversity in financial flows and clients (including a large share of private banking and fund transactions)
  - This may increase complexity to identify beneficial ownership of TCSPs clients, source of funds and understanding the activities they conduct
- The presence of many legal entities and arrangements(137 444 entities registered with the RCS in Luxembourg as of June 2020);
- The use of intermediaries/third parties to conduct a range of activities, from initial introductions to clients to advisory specific topics, and over relying on those intermediaries to fulfil their obligations, and non-face-to-face transactions.

Table 27 provides an overview of the vulnerability assessment per assessment dimension, further detailed in the section below.

Table 27: Overview of inherent risk factors of TCSP activities per assessment dimension

Assessment dimension	Inherent risks
Structure	• Complex sectoral structure, including a large number of entities providing TCSP services, supervised by different authorities and SRBs
Ownership	• Complex ownership of entities providing TCSP services, which may have a high number of foreign owners
Geography	• Exposure to multiple jurisdictions, reflecting the attractiveness of Luxembourg as an international financial centre • This may increase complexity when it comes to identifying beneficiary ownership of TCSPs clients, source of funds and understanding the activities they conduct

[528] FATF (2019), Guidance for a Risk-Based Approach for Trust & Company Service Providers (TCSPs), FATF, Paris, www.fatf-gafi.org/publications/documents/rba-trust-company-service-providers.html. The guidance describes three dimensions instead of five, namely 'Country/Geographic risk', 'Client risk' and 'Transaction/service and associated delivery channel risk'

Assessment dimension	Inherent risks
Products / activities	• TCSP activities relating to the set-up of entities, including incorporation, domiciliation and nominee shareholder services have a high ML/TF inherent risk due to products and services potentially being abused or misused to create complex networks of structures to conceal the identity of criminals • TCSP activities relating to the management of a client's activities, including fiduciary/trustee services, and the provision of directorship, have a high ML/TF risk due to products and services being abused or misused by criminals to distance themselves from ML/TF activities (liability with the TCSP provider) • Secretarial services are relatively lower risk, given clients retain responsibility for actions taken and do not transfer it to TCSPs, limiting criminals' ability to conceal their identity
Clients/ transactions	• TCSP activities relating to the set-up of entities, including incorporation, domiciliation, and nominee shareholder services are highly exposed to complex and sophisticated clients and a significant level of intermediation increases ML/TF risks • TCSP activities relating to the management of a client's activities, including fiduciary/trustee services, and the provision of directorship services, are highly exposed to complex and sophisticated clients, which often have limited reporting requirements, and a significant level of intermediation
Channels	• TCSPs often use intermediaries/ third parties to conduct a range of activities, from initial introduction to clients to advisory on specific topics. These intermediaries/third parties may increase exposure to ML/TF risk

Detailed vulnerability assessment of TCSP inherent risk per scorecard dimension

Given the data and information on the proportion of TCSP activities provided by the many entities outlined as above, we refer the reader to the specific structural and ownership assessments of entities providing TCSP activities in relevant sections of the NRA. In line with a conservative approach, it is estimated that diversity and fragmentation of the structure and ownership levels to be a driver of risk, based on an aggregate assessment of threat levels of the various entities on these dimensions.

Structure and ownership

As previously described, TCSP services are provided by a wide range of entities, including sectors supervised by the CSSF, the CAA, the AED and SRBs. This creates a sizeable and complex landscape, particularly when considering the number and size of entities that could provide TCSP activities. For SRB-regulated entities, this includes 1 173 chartered professional accountants, 581 statutory auditors, 78 audit firms and 2 917 lawyers in Luxembourg in 2019, but not all of them providing TCSP services in addition to their core activities.

While TCSPs within the financial sector are predominantly in the market leading, large TCSPs, there is a "long-tail" of smaller TCSPs in Luxembourg conducting set-up activities. This level of fragmentation increases exposure to ML/TF risks. Particularly worth noting in this context is the sub-sector risk of specialised PFSs, which in Luxembourg, is driven by their significant size. There are 92[529] specialised PFS entities providing trust and company services[530] with 4 478 employees[531]as of December 2019 with balance sheet assets of €0.8 billion[532] and profit of €77 million[533]. The market has a relative degree of complexity as specialised PFSs can include various types, each offering different services. Those types include registrar agents, corporate domiciliation agents, professionals providing company

[529] Including the three support professionals of the financial sector providing TCSP services
[530] CSSF *data*, 2019
[531] CSSF *data,* 2019
[532] CSSF *data*, 2019
[533] CSSF *data,* 2019

incorporation and management services, family offices and administrative agents of the financial sector. The risks are mitigated by the relative concentration of the sector, as the five largest entities in the sub-sector account for approximately 40% of all revenues.

Similar to other activities, there is a "long-tail" of smaller professionals; however, certain activities are characterised by large economies of scale, which therefore leads to higher concentration in the provision of administration activities. Additionally, on the TCSPs' end, administration activities involve handling a significant number of administrative tasks and transactions, which can increase the volume and complexity of services provided.

By way of aggregation of vulnerabilities of the separate entities, the ownership structure of entities providing TCSP services is deemed to significantly expose TCSPs to ML/TF risks.

Geography

As an international financial centre, Luxembourg is exposed to business originating from multiple jurisdictions, and the TCSP industry is no exception. TCSPs' corporate clients are generally multinationals based outside of Luxembourg, typically from the US or the European Union.

While such geographic exposure reflects the attractiveness of Luxembourg as an international financial centre, it may increase complexity when it comes to identifying beneficiary ownership of TCSPs clients, source of funds and understanding the activities they conduct.

Due to this complexity, it is important to note that TCSPs are geographically exposed through several channels. In this respect, the exposure spans not only the origination of Luxembourg's TCSP clients, but also the beneficial owner of the latter and identified client politically exposed persons (PEPs).

As defined under the 4th Anti-Money Laundering Directive (4AMLD), third parties (e.g. Know-Your-Customer (KYC)/Customer Due Diligence (CDD) service providers) that perform activities falling within the scope of the 2004 AML/CFT Law must be regulated in a country with equivalent AML/CFT standards as Luxembourg. Thus intermediaries are typically not required to be registered or supervised in Luxembourg as they are regulated and supervised in their country of origin. However, where CDD is outsourced, the outsourcing entity maintains responsibility for compliance with the professional obligations set out in the 2004 AML/CFT Law (see Article 3-3).

Additionally, the nature of the TCSPs business itself generates a geographic exposure. The TCSP sector is inherently international, with activities often expanding multiple geographies.

Products/activities

Under Luxembourg's law, it is not a requirement that a TCSP is directly involved in a company's incorporation. The nature of ML/TF risks relating to the provision of these services is related to the ways in which a criminal may abuse or misuse this service to set up a complex network of structures that permits the concealment of their identity and the source of the funds. Notwithstanding, the setup of structures in the form of unregulated legal entities has a higher associated ML/TF risk. Unregulated legal entities tend to have less stringent reporting requirements, fewer limitations with regards to the assets, which they can hold and/or invest in and have lower risk diversification requirements.

TCSP services related to the management of an entity, for example the provision of fiduciary/trustee services and directorship, may be particularly exposed to ML/TF risk. This arises from the potential for criminals to abuse or misuse the advice provided by TCSPs to design and implement complex schemes and conceal their identity by delegating decision-making power to TCSPs[534]. By providing activities relating to the management of an entity, TCSPs have the power to advise and execute decisions relating to the structure being managed. As such, TCSPs permit clients to navigate complex fiscal and

[534] FATF and Egmont Group, *Report on Concealment of Beneficial Ownership*, 2018

reporting requirements in place, for example by understanding and designing structure to manage their assets based on the jurisdiction's requirements. Importantly, when managing these structures, TCSPs become liable for the decisions and actions of the client. Therefore, the TCSP will be registered as the originator or approver of decisions and actions conducted by the professional, even in instances where client instructions were being followed. However, for example for directorship services, the TCSP (or the individual within the TCSP appointed as director) is liable for any actions they approve, and thus has the incentive to ensure an appropriate level of controls are applied over actions and transactions they are approving. This may somewhat reduce the level of exposure to ML/TF risk.

Secretarial services are typically less vulnerable to ML/TF. They generally involve the execution of back-office activities that have limited overlap with actions typically carried out with the purpose of laundering illicit funds. Nevertheless, clients maintain responsibility over decisions and actions executed by the structure. As such, clients or their BOs will be recorded as the originator or approver of decisions, hence limiting the opportunities to conceal their identity. Therefore, potential for administration services to be abused or misused for ML/TF purposes is limited, compared to setup and management. Still, while relatively limited, there may be instances, such as the use of administrative services to give substance to the company, in which criminals are able to abuse or misuse administration services provided by TCSP.

Clients/transactions

ML/TF risks resulting from client segments are determined by the profile of these clients. As an example, in the case of the financial sector, private banking clients often have a sophisticated financial profile (e.g. they may hold illiquid and complex assets like real estate) and typically have limited disclosure requirements regarding their activities, which may result in higher level of complexity for a TCSPs and thus of ML/TF risk exposure. In line with this, large corporate clients may have complex ownership and management structures, and SMEs in general do not have as strict reporting requirements as larger firms. This in turn, may result in a reduction in the transparency of corporates' BOs and activities.

Additionally, TCSPs clients have heterogeneous legal structures, and the use of complex legal structures may be a challenge for TCSP. These structure types may increase the level of complexity when it comes to identifying and understanding its management and beneficiary structures.

As previously mentioned, secretarial activities tend to have less exposure to private clients, and these administrative activities are less exposed to ML/TF risks compared to set-up and management activities.

Channels

TCSPs often use third parties to conduct a range of activities, from initial introduction to clients, either via introducing intermediaries whose role is to connect clients and TCSPs, or via clients' advisers, which represent their interest and are the direct point of contact for the TCSP, to advisory on specific topics. Though uncommon in Luxembourg, TCPSs may rely on or use the assistance from these third-parties when performing their CDD requirements; while the ultimate responsibility of the CDD lies with the TCSP, this level of intermediation may result in exposure to AML/CFT risks.

Beyond the presence of third parties, activities relating to the set-up of an entity can be offered through direct and remote channels to offer their products to clients (e.g. online, over the phone). The use of remote channels can affect the ability of professionals carrying out TCSP activities to accurately verify the identity of clients and their BOs.

6.4.2. Cash

The usage of cash for ML/TF purposes is considered as an important vulnerability internationally and in Luxembourg. Cash remains a primary means of transaction across the globe for legitimate purposes, and is predominant in low value payments, though customer habits and preferences differ across countries, with ~80% of point of sale transactions being carried out using cash, amounting to ~54% of the total value of all payments[535]. Hoarding of cash is a known habit, yet it is difficult to quantify. However, cash is also believed to be a key asset in criminal activity, particularly in organised crime group's (OCG) activities (e.g. drug trafficking, goods smuggling, prostitution), constituting a significant part of OCGs' portfolio[536]. Criminals tend to target cash intensive businesses for laundering money and attempt to channel cash through the legitimate financial system.

The level of net annual cash issuance in Luxembourg has been decreasing since 2014. Net annual issuance refers to the net amount of cash issued in a given year, which is calculated as the difference of the cumulative cash issued for two consecutive years. To understand the level of cash usage in Luxembourg, it is possible to compare the net annual issuance of euro banknotes in Luxembourg with the rest of the Eurozone and assess whether this is in line with other financial indicators (e.g. Luxembourg's share of banking assets, level of outstanding debt securities and GDP). It must be noted, however, that a given share of the Eurozone sum may appear disproportionate since the annual issuance in a certain year of some countries may be very low. Net annual issuance of euro banknotes in Luxembourg has decreased since 2014 to ~1-2% of whole Eurozone issuance, and is in line with Luxembourg's share of both banking assets (~3% of Eurozone), and of the total outstanding value of debt securities issued (~4% of Eurozone), as shown in the table below. The decreasing issuance of cash in Luxembourg coincides with the adoption of key measures on international exchanges of information, such as the EU's automatic exchange of information[537], and OECD's Common Reporting Standard[538] against which Luxembourg was rated as "Largely Compliant" in 2018[539].

Table 28: Net annual issuance of Euro notes in Luxembourg (LU) and other Eurozone countries

		2014	2015	2016	2017	2018
Net annual issuance of euro banknotes[540]	LU (€ billion)	6	2	1	1	1
	Eurozone (€ billion)	60	67	43	45	60
	LU share of Eurozone (%)	10%	3%	3%	2%	1%
Banking assets[541]	LU share of Eurozone (%)	3%	3%	3%	3%	4%
Debt securities (amount outstanding)[542]	LU share of Eurozone (%)	4%	5%	5%	5%	5%
GDP[543]	LU share of Eurozone (%)	0.4%	0.4%	0.4%	0.4%	0.4%

[535] G4S, *World Cash Report,* 2018 (link)

[536] European Commission, *Organized Crime Portfolio Project*, 2015 (link)

[537] From 2014 onwards, the communication of (end of year) cash account balances had become automatic.

[538] See OECD for further information (link)

[539] OECD, *Global Forum on Transparency and Exchange of Information for Tax Purposes: Luxembourg 2019,* 2019 (link)

[540] Banque Centrale du Luxembourg, *Rapport Annuel*, 2014 – 2018

[541] ECB MFI Balance Sheet

[542] Bank for International Settlements – debt securities issued by resident issuers, amount outstanding as of Q4 of each year

[543] Eurostat

In previous years, it has been suggested that the level of cash usage was relatively high in Luxembourg. For example, a EUROPOL report[544] published in 2015 indicated specifically that Luxembourg was one of the main issuers of euro banknotes and that this issuance was disproportionate. The level of cash issuance was portrayed as at odds with perceived usage and outflows. However, this report focused on stock (cumulative net issuance[545]) and not flow (net annual issuance), which limits understanding of the impact of recent evolutions (e.g. new regulations), as demonstrated above.

Notwithstanding this, the ML/FT risks resulting from the use of cash in Luxembourg should still be considered by public and private entities. The number of border cash declarations (relating to currency and other bearer negotiable instruments) received by ADA has remained relatively stable over the past five years, as highlighted in the table below. The total value of cash border declarations made in 2018 (€5.4 million) represents less than 1% of the total value declared to customs authorities across the Eurozone in the same year (€51 billion).[546]

Table 29: Border cash declarations (relating to currency and bearer negotiable instruments) 2015-2019, including both intra-EU and extra-EU cash transport

		2014	2015	2016	2017	2018	2019
EU regulation[547]	Number of declarations	59	51	32	43	24	51
	Associated value (€)	1 666 062	1 869 103	93 731 211	1 304 319	736 724	1 168 759
National legislation[548]	Number of declarations	145	144	62	119	132	154
	Associated value (€)	3 843 435	5 521 279	3 551 438	1 933 000	4 677 049	16 328 960

Finally, FATF has also noted in its guidance on the impact of COVID-19 on ML/TF that recent swings in securities values are resulting in individuals liquidating their portfolios, and that there has been an overall increase in banknote withdrawal, with some FATF members raising withdrawal limits.[549] The reason for the increase has not been analysed as part of this exercise, but this may be due to a fear of bank failures based on experience from previous crises. Though this development is not Luxembourg specific it can lead to additional cash usage in Luxembourg as well.

The prevalence of cash and level of cash usage pose ML/TF risks in Luxembourg, given that the use of cash can mask ML/TF activities. There are several typologies that indicate the ML/TF challenges associated with cash, including (but not limited to):

- Ease of transport cross-border by exploitation of cash declaration systems and EU open borders, and/or smuggling via cargo freight and mail;
- Usage of high-denomination bank notes (€500, €200);
- Counterfeiting currency (most commonly lower denomination notes). It should be noted, however, that the number of counterfeit euro banknotes in circulation across Europe remained

[545] Referring to the stock of cash issued since the beginning of the Eurozone in a given year

[546] See Europa.eu (link)

[547] This refers to the obligation of declaration once the cash crosses the external border of the EU

[548] This refers to the obligation of declaration once the cash crosses an EU border

[549] FATF, *COVID-19-related Money Laundering and Terrorist Financing*, 2020 (link)

low in 2019 and has continued to decrease since 2014. Compared with the number of genuine euro banknote in circulation, the proportion of counterfeits is very low)[550];

- Re-depositing of large amounts of cash to cover the laundering of illicit funds;
- Being used to purchase "safe haven" assets (e.g. gold) which are less easily traceable; and
- Being used in "cash-out" schemes where criminals obtain access to an individual's bank account and withdraw funds in banknotes from an ATM.

It should also be noted that some sectors are particularly exposed to ML/TF risks associated with cash, due to specific characteristics of the sector (e.g. being cash-intensive). For example:

- Dealers in goods, particularly high-value goods which offer criminals an easy way to launder illicit funds;
- Money and value transfer services, which may operate through a global network of agents, present vulnerabilities concerning ML;
- Real estate activities, where schemes could include under or over-valuation of properties (which may allow criminals to purchase an asset below market price and pay the different to the seller in cash); and
- Casinos and other entities associated with gambling are typically cash-intensive, often operating 24 hours per day with high volumes of large cash transactions taking place very quickly, even though in Luxembourg there is only one casino and other gambling activities are deemed low ML/TF risk.

[550] European Central Bank, *Annual Report*, 2019 (link)

6.4.3. Virtual assets

Over the past five years, virtual assets (VAs) became increasingly adopted for various legitimate activities, for example, for investments or transactions. VAs have unique technological properties that enable pseudo-anonymous and anonymous transactions, fast cross-border value transfer and non-face-to-face business relationships. Those properties have the potential to improve multiple financial products and services such as trade financing, cross-border payments and financial instrument settlement. Traditional financial institutions have recognised those benefits. For example, a survey by the Bank for International Settlements of 63 central banks in 2018 showed that most of them were analysing the possibility to issue central bank-backed VAs[551]. Furthermore, VAs market adoption rate has been increasing globally. The number of VAs with at least a $1 million market capitalisation has risen from 30 to approximately 1 000 between 2015 and 2020, with a combined capitalisation of all VAs approaching $300 billion[552].

At the same time, the same features of VAs that drive legitimate adoption, also make them vulnerable to abuse by criminals for ML/TF activities. Globally, in 2019 more than $10 billion worth of VAs were used for ML purposes[553]. VAs can be misused by criminals to facilitate transactions on illegal products marketplaces and investment fraud schemes, the combined revenues of which exceeded $1 billion in the same year[554]. VAs are also increasingly used by terrorist financing groups, cybercriminals and sexual exploitation profiteers[555]. Given the high volatility of VAs, VAs could be prone to speculative bubbles, and there have been suspected cases of market manipulation in VA markets[556].

The high adoption of VAs by criminals poses significant challenges for virtual asset service providers (VASPs), i.e. entities that facilitate VA transactions (e.g. dedicated VA custodians, VA exchanges), entities of other sub-sectors, supervisors and law enforcement agencies.

Globally, several jurisdictions and international bodies have recognised the rising ML/TF threat of VAs and VASPs. FATF highlighted virtual currencies as one of the key emerging risks to ML and TF, and in particular offences of tax evasion and fraud[557]. The EU Supranational Risk Assessment recognised Vas' and VASPs' rising risk to ML/TF purposes[558]. Further, some countries have explicitly analysed the vulnerability of VAs and VASPs and published correspondent risk assessments, highlighting the threat of VAs being misused or abused for terrorist financing, investor fraud, drug trafficking and other predicate offences[559] Note that as of July 2020, Luxembourg authorities are in the process of conducting a separate vertical risk assessment on VASPs.

The technological and market factors of VAs and VASPs imply that proceeds from all predicate offences, identified in the NRA, can be potentially laundered through them. Threats that may be particularly increased by VAs include drug trafficking, fraud and forgery, and terrorist financing.

The VA space is relevant to drug trafficking in two significant ways. First, proceeds from drug trafficking can be laundered through VASPs. Criminals can generate drug-trafficking revenue in fiat, convert that fiat into VAs, and then exchange VAs back into fiat currency. Second, VAs can be used as part of the

[551] The Bank of International Settlement, "Proceeding with caution – a survey on central bank digital currency", January 2019

[552] Coinmarketcap, https://coinmarketcap.com/, retrieved 14 February 2019

[553] Ciphertrace, Q3 2019 Cryptocurrency Anti-Money Laundering Report, November 2019

[554] Ciphertrace, Q4 2019 Cryptocurrency Anti-Money Laundering Report, February 2020

[555] Chainalysis, 2020 Crypto Crime Report, January 2020

[556] Neil Gandal, JT Hamrick, Tyler Moore, and Tali Oberman, Journal of Monetary Economics, *Price Manipulation in the Bitcoin Ecosystem*, 2017

[557] FATF Report, *Virtual currencies – key definitions and potential AML/CFT risks*, June 2014

[558] European Union Supranational Risk Assessment Update, July 2019

[559] For example: Swiss Interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism (CGMF), *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, 2018

criminal offence itself as a medium of exchange. Multiple online "darknet" markets exist that connect drug buyers and sellers, in which trade can be facilitated with VAs.

Fraud generally refers to investment frauds, scams and phishing. VAs can potentially enable those threats as they allow criminals to remain pseudo-anonymous in their operations. Globally, the total monetary amount of investment frauds, which use VAs in their operations, has reached $4 billion volume in 2019. The majority of those funds are linked to Ponzi schemes, which counted 2.4 million individual transactions. Luxembourg's position as an investment hub increases the probability that criminals can abuse or misuse the investment sector to conduct fraud. While no known large-scale Ponzi or investment schemes were operated from Luxembourg, multiple fraudulent VASPs falsely claimed they were regulated there. Criminals were abusing Luxembourg's reputation for having a stable investment and regulatory environment. In this context, the CSSF has issued warnings on four entities, falsely claiming to have a license in Luxembourg (one case in 2018, two in 2019 and one in 2020), including an investment scam and a fake exchange[560].

VAs also represent a potential alternative to fiat currency for terrorist financing. VAs can be misused by terrorist organisation donors to give donations pseudo-anonymously and avoid sanctions. According to a report published by The Middle East Media Research Institute, the list of terrorist organisations that have received donations in Bitcoin include ISIS, Al-Qaeda, Hamas and the Muslim Brotherhood[561].

Given that VAs can be misused by criminals to launder proceeds obtained during predicate offences, or be misused as part of an offence itself as a medium of exchange, entities from different sub-sectors may be potentially exposed to ML/TF risks related to VAs by interacting with VASPs. Firms from the following industries have the highest likelihood of being directly or indirectly exposed to those ML/TF risks:

- **Banks**: Banks are exposed to VAs risk as they are the point of contact of centralised exchange users with the traditional finance sector. Criminals using VAs for ML/TF activities need to convert VAs to fiat, or vice-versa. For that, criminals use exchanges, the deposits and withdrawals from which are usually done to and from bank accounts. Luxembourg has a substantial retail and business bank sector, with large numbers of existing customers, including a high share of international users. As of 2019, no bank in Luxembourg had itself business activity in VAs, with a small minority of banks (less than a dozen) having a very limited number of customers involved or linked to VAs. Thus, the VA-related ML/TF risks to banks in Luxembourg are limited.

- **Money and value transfer services**: E-money institutions and payment institutions may be exposed to VASP-related ML/TF risk by enabling their users fiat deposits and withdrawals to and from different VASPs, such as VA exchanges. Two payment institutions in Luxembourg provide services involving VAs and are supervised by the CSSF as licensed payment institutions for the payment activities linked to the VAs activities. The VAs activity itself is currently under assessment by CSSF pursuant to the new framework provided for in Article 7-1 of the 2004 AML/CFT Law.

- **Insurance:** VA exchanges and custodians require insurance to secure their operations. Globally, there has been a rise of insurance providers to custodians. For example, in 2019 Marsh, an international insurance broker, arranged a $150 million insurance policy from Lloyd's to insure a custodian solution provider form hacks and thefts[562]. Insurers need to be able to analyse

[560] CSSF, *Warning concerning the website www.crypto-bull.io*, 2020 (link)
CSSF, *Warning concerning the website http://fundrockcrypto.com*, 2019 (link)
CSSF, *Warning regarding the activities of an entity named Cryptominingoptionsignal*, (link)
CSSF, Warning regarding the activities of an entity named Cryptofinance, 2018 (link)
[561] Middle East Media Research Institute, The Coming Storm – Terrorists Using Cryptocurrency, August 2019
[562] Marsh, Blue Vault: An Innovative Cold Storage Solution for Digital Assets, 2019

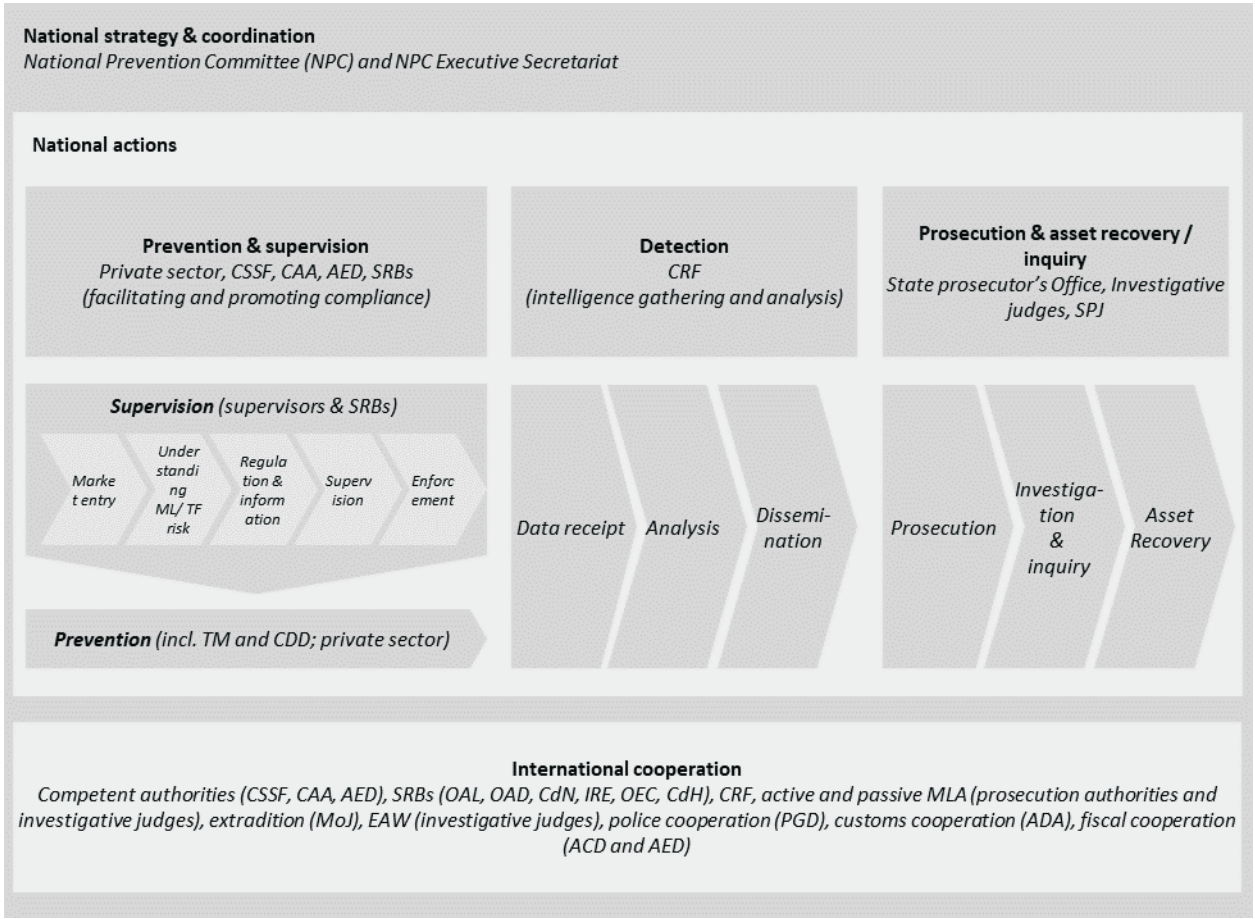
cybersecurity threats effectively, as VA custodians can be a target of cyber criminals. Note that the insurance coverage of VAs is very limited globally[563], which thus also constraints the risk to the Luxembourg insurance sector.

[563] American Express, *Cryptocurrency Insurance Market Shows Promise Despite Cautious Approach by Major Insurers*, 2018

7. MITIGATING FACTORS

This section outlines the mitigating factors of the agencies involved in Luxembourg's national AML/CTF framework. As described in the methodology section, the mitigating factors are described across five main components as per the framework depicted in the figure below. Relevant agencies under each component are described along a common set of dimensions along mandate, model, capabilities and results, with various degrees of detail depending on the role played by the agency in the national AML/CTF framework. The relevant illustrations from the methodology section are included here for ease of reference.

Figure 14: Mitigating factors framework

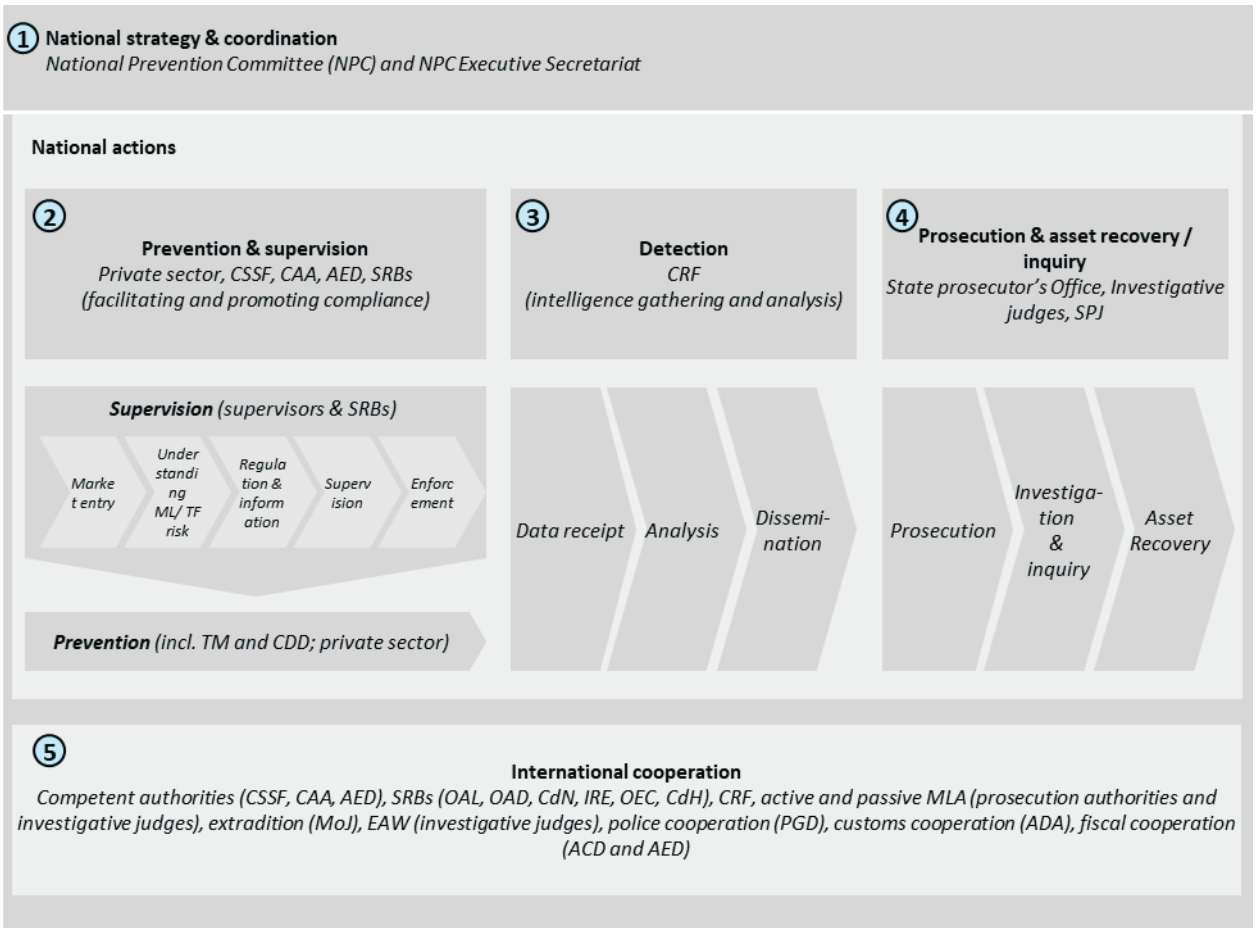


7.1. Overview of mitigating factors

Luxembourg has established an effective AML/CFT regime based on a solid legal framework and a comprehensive institutional set-up involving a wide range of competent authorities to prevent, supervise, detect, investigate and prosecute ML/TF, and to recover assets. The national AML/CFT framework effectively mitigates the inherent risks detailed in the previous sections, as reflected in the resulting residual risk (see the following section).

The NRA assessed Luxembourg's AML/CFT regime against the five dimensions shown in the figure below: national strategy and coordination, prevention and supervision, detection, prosecution and asset recovery, and international cooperation. The following stakeholders were involved in this assessment: ministries (Finance, Justice, Foreign Affairs), national supervisors and administrations (CSSF, CAA, AED, ACD, ADA, LBR), the financial intelligence unit (CRF), law enforcement entities (prosecution authorities, Investigative Judges, the Judicial Police Service) and Self-Regulatory Bodies (OEC, IRE, OAL, OAD, CdN, CdH).

Figure 15: Mitigating factors framework



The **Comité national de prevention du blanchiment et du financement du terrorisme (NPC) and its dedicated Executive Secretariat** play a central role in setting the strategic direction for the national AML/CFT framework and coordinating the national actions. The NPC defines, coordinates and oversees the implementation of the national AML/CFT strategy. It is supported by a permanent Executive Secretariat in charge of coordinating the efforts of the NPC, e.g. by scheduling, organising and preparing NPC meetings, leading the update of the NRA and the national AML/CFT strategy and monitoring the implementation of the strategy across agencies. The NPC drafted and published the update of the National Risk Assessment (NRA) at the end of that year. The NRA exercise included the

formulation of the national AML/CFT strategy, which defined national strategic priorities, a national action plan and agency-level action plans. Over the course of 2019 and 2020, the NPC and the Executive Secretariat oversaw and coordinated the implementation of the national AML/CFT strategy, including: the preparation of legislative work to create and organise an Asset Recovery Office (ARO), create new databases and retrieval systems (e.g. BO registers, bank account and deposit box retrieval system) and the transposition of the 4th and 5th AMLD. In 2020 the NPC performed the update of the NRA and the national AML/CFT strategy and conducted several vertical risk assessments (i.e. virtual assets service providers, legal entities & arrangements and terrorist financing).

Luxembourg's AML/CFT supervisors ensure that the private sector effectively implements their AML/CFT obligations. In 2019, AML/CFT competent supervisors in aggregate undertook over 250 on-site inspections and over 500 desk-based reviews, enforced over 90 remedial actions (in the form of warnings, reprimands, fine, etc.), and published over dozens of guidelines (e.g. 15 circulars).

The **Commission de Surveillance du Secteur Financier (CSSF)** is the financial sector's prudential and AML/CFT supervisory authority. The CSSF supervises a broad range of financial sector professionals, including: banks, payment and e-money institutions, agents and e-money distributors acting on behalf of payment and e-money institutions established in other European member states, investment firms, collective investments, specialised and support PFSs and market operators. Since March 2020, the CSSF is also the AML/CFT supervisory authority for virtual asset service providers (VASPs) established or offering their services in Luxembourg. The CSSF has strict market entry controls, such as licensing, registration and authorisation requirements (e.g. fit and proper requirements, analyses for recommendation of authorisation to the Ministry of Finance), which includes ongoing review (e.g. upon change of shareholders). The CSSF has the power to revoke licenses or registrations for non-compliance (on AML/CFT matters or other). Additionally, there is a common authorisation process in place since November 2014, with Euro-zone banks being under ultimate licensing authority of the European Central Bank (ECB).

The CSSF disposes of a wide range of supervisory powers, including requesting and accessing information from supervised entities, exchanging information with other national and international authorities, carrying out on-site and off-site inspections and investigations, imposing sanctions and requesting freezing or seizure of assets with the prosecution authorities. In 2019, the CSSF conducted 57 on-site inspections and issued administrative fines worth 140 000 euros[564] strictly related to on-site inspections performed in 2019. The sanctioning powers are harmonised across the different sub-sectors under CSSF's supervision. The CSSF also established a whistleblowing process to encourage and promote identity protection of whistle-blowers. Different teams within CSSF participate in AML/CFT activities, including supervisory teams and dedicated AML/CFT on-site and off-site inspection teams, the Legal team and committees to discuss cross-cutting issues. A dedicated central coordination team supports these teams, which ascertains a harmonised and coordinated approach across CSSF.

The CSSF applies a risk-based approach to AML/CFT supervision, which also applies to internal procedures (e.g. to prioritise resource allocation). The CSSF promotes awareness and education in the sectors it supervises by issuing circulars (six AML/CFT-specific circulars in total in 2018-2019) and circular letters to complement or clarify AML/CFT regulations. The CSSF also conducted and published detailed sub-sector risk assessments on private banking[565], collective investments[566] and specialised

[564] 2019 administrative fines data are not final

[565] CSSF, *ML/TF sub-sector risk assessment: Private Banking,* 2019

[566] CSSF, *ML/TF sub-sector risk assessment: Collective Investments,* 2020

PFSs providing corporate services (TCSP activities)[567]. The CSSF established two sector-specific AML/CFT Expert Working Groups. In 2019, the CSSF organised multiple AML/CFT conferences for the sub-sectors it supervises, including dedicated conferences for banks, specialised PFSs, investments firms, payment, e-money institutions and agents and e-money distributors acting on behalf of payment and e-money institutions established in other European Member States, and collective investments. Different employees from the CSSF also participated as speakers in AML/CFT conferences organised by the financial sector. During all these conferences the CSSF addressed topics including on-site and off-site supervision findings, entity-level risk assessments and regulatory evolution. The CSSF has cooperation and information exchange frameworks in place with other national and international authorities. It is further enhancing such processes in particular in relation with the implementation of the AML/CFT colleges in line with the Joint guidelines on cooperation and information exchange for the purpose of the 4th AML Directive between competent authorities supervising credit and financial institutions[568].

The **Commissariat aux Assurances (CAA)** is the insurance sector's prudential and AML/CFT supervisor (including insurers, reinsurers, intermediaries, professionals of the insurance sector and CAA-supervised pension funds). The CAA has strict market entry controls through licensing and authorisation requirements (890 applications in 2019, of which 321 were rejected), has the power to request and access information and to penalise non-compliant entities (with sanctions including fines, penalties, other remedial action orders or blocking certain actions such as acquisitions). In 2019 the CAA conducted 415 desk-based reviews and 41 on-site inspections (of which 14 had an AML/CFT component) and used a risk-based approach to prioritise them. Following on-site inspections, the CAA issued 38 injunctions for non-compliance with AML/CFT obligations. The CAA focuses on increasing awareness of ML/TF risks and AML/CFT obligations among its regulated entities. For instance, in 2019 the CAA issued 10 AML/CFT specific circular letters as well as two regulations, which include some specific guidance related to AML/CFT training and the issuance of a special report by the independent auditor. The CAA also organised an AML/CFT conference in 2019, during which it addressed various topics including the NRA, the AML/CFT risk-based approach, financial sanctions in the framework of TF and CAA's different AML/CFT inspection types. The CAA has data exchange in place with other national and international authorities.

The **Administration de l'Enregistrement, des Domaines et de la TVA[569] (AED),** Luxembourg's tax administration in charge of indirect taxes (e.g. VAT, stamp duty, succession taxes, registration fee), is the AML/CFT supervisor for real estate agents, accountants and tax advisors, some TCSPs, such as business centres and directors, gambling establishments, freeport operators and some dealers in high value goods[570]. The AED supervision is focused on Designated Non-Financial Businesses and Professions. Since February 2018, the AED has the same supervisory powers as the CSSF and the CAA. In accordance to the 2004 AML/CFT Law, it has a wide range of sanctions available, including warnings, reprimands, public statements and fines. In carrying out its supervisory mission, the AED has access to databases for which it is responsible for processing, but can also request any information useful to its function as AML supervisory authority, more particularly in carrying out its inspections. For AML/CFT purposes, the AED has data-sharing protocols (MOU) with a variety of national authorities.

The AED has a dedicated AML/CFT unit and dedicated staff for running AML/CFT inspections in the anti-fraud Unit. The AML/CFT unit is frequently involved in the legislative process leading to rules to supervised professionals or sectors. During on-site inspections, dedicated agents from the Anti-fraud

[567] CSSF, *ML/TF sub-sector risk assessment: Specialised PFS providing corporate services (trust and company service provider activities),* 2020

[568] Joint guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions, No JC 2019 81 » of 16 december 2019

[569] Registration Duties, Estates and VAT Authority

[570] Natural or legal persons trading in goods, only to the extent that the payments are made in cash in an amount of €10.000 or more whenever a transaction is executed in a single operation or in several operations which appear to be linked.

unit perform checks on customer due diligence practices, adequacy of internal management, risk assessments performed and on cooperation with AML/CFT authorities. In 2019, the AED performed 82 on-site inspections and issued 58 fines for a total value of €622 750, with an average fine equal to ~€10 600. For the prevention and awareness component of the AED supervision mission, the AED engages with the private sector through bilateral meetings, trainings, conferences, sending questionnaires to supervised entities and publishing circulars. In 2018, the AED also published four separate guides on professional obligations in the fight against ML and TF for most of its supervised sub-sectors: accountants and tax advisors, dealers of goods, real estate and TCSPs.

Legal professions, chartered accountants and auditors in Luxembourg are **supervised by dedicated self-regulatory bodies (SRBs) for AML/CFT** purposes, namely (approved) statutory auditors *("réviseurs d'entreprises (agréés)")*, (approved) audit firms *("cabinets de revision (agréés))*, chartered professional accountants *("experts-comptables")*, notaries *("notaires")*, lawyers *("avocats")* and bailiffs *("huissiers de justice")*. As defined in the 2004 AML/CFT law, all SRBs are subject to the same overarching AML/CFT obligations: ML/TF risk assessment, customer due diligence, adequate internal organisation and cooperation requirements with the authorities. While supervisory powers are broadly aligned across the SRBs, some powers and practices may differ, reflecting specificities of their profession. Most SRBs have published AML/CFT standards for their supervised professionals, which they update on a regular basis if AML/CFT requirements change (i.e. IRE, OEC, CdN, OAL, OAD, CdH). SRBs regularly organise trainings on AML/CFT topics for supervised professionals, some of which are together with the director of the CRF (e.g. OAL/OAD and CdN). Some SRBs (such as IRE and OAL) have established a formal whistleblowing process. As of 2020, most SRBs (i.e. IRE, OEC, CdN, OAL, CdH) have started implementing a more formalised consistent risk-based approach that assesses entity-level risk based on information obtained via an annual AML/CFT questionnaire sent to their supervised professionals. SRBs conduct reviews performed by controllers employed by the SRBs and peer reviewers. SRBs may sanction supervised entities for non-compliance with their AML/CFT obligations. The 2020 amendments of the 2004 AML/CFT law aligned the supervisory and sanctioning powers across SRBs. In practice, SRBs focus on following up inspections that have found deficiencies.

A range of professions in Luxembourg are authorised to conduct at least one (or more) of what the 2004 AML/CFT Law defines as **trusts & Corporate Service Providers (TCSPs)** activities. Several factors are in place to mitigate the risks of TCSP services. First, all the professionals that provide TCSP services are supervised on AML/CFT by one of Luxembourg's competent authorities (CSSF, CAA, AED) or self-regulatory bodies (OAL, OAD, IRE, OEC). All professionals providing TCSP services need to follow the AML/CFT professional obligations under the 2004 AML/CFT Law and, as of March 2020, are required to register with the related competent authority or SRB. Lastly, competent authorities, self-regulatory bodies and other national agencies have taken specific measures to mitigate the ML/TF vulnerabilities of TCSPs and TCSP activities, including for example questionnaires drafted by SRBs for their supervised professionals (lawyers, auditing profession and chartered professional accountants), which were sent out between February and May 2020.

Several factors contribute to mitigating ML/TF risks for Luxembourg's **legal entities and arrangements**. All **legal entities** incorporated in Luxembourg must be registered with the **Registre de commerce et des sociétés** (RCS). The RCS counts 165 869 legal entities in the registry as of February 2020. Information available in the registry slightly differs by type of company. As of 2019, the RCS is managed by the **Luxembourg Business Register** (LBR). As per the Beneficial Ownership law[571], all legal entities – with the exception of sole traders and Fonds d'investissements alternatifs réservés (FIAR) – are under the obligation to fill out the newly created **Registre des bénéficiaires effectifs** (RBE) register with ultimate beneficial ownership information. In line with 5th AMLD requirements on BO registry, the RBE is "accessible in all cases to competent authorities and the CRF; […] obliged entities […]; any

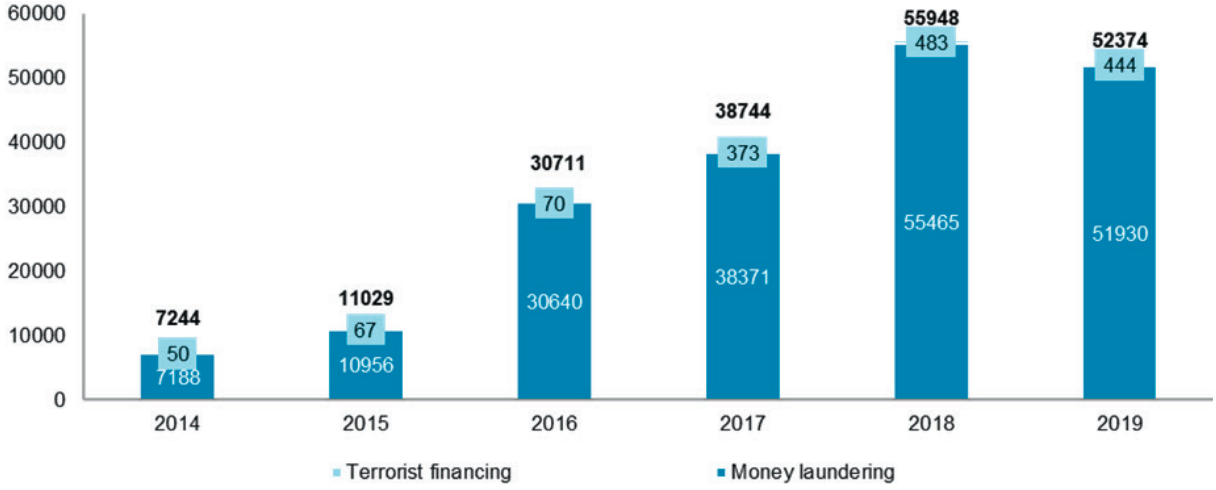
[571] January, 13th 2019

member of the general public[572]" and includes "the details of beneficial interests held." **Legal arrangements** are not registered at the RCS, however in line with the 4th AMLD, a centralised database of beneficial ownership of fiducies and foreign trusts has been established under the AED by the Law of 10 July 2020.

Detection activities are primarily driven by Luxembourg's financial intelligence unit, the **Cellule de renseignement financier (CRF)**. Its responsibilities include receiving and analysing AML/CFT information and disseminating the intelligence it gathers to the relevant authorities. The CRF is an independent agency headed by magistrates who operate independently and autonomously. The administrative independence of the CRF was established in 2018: Before, the CRF sat within the State Prosecutor's Office at the Luxembourg District Court. Magistrates of the CRF carry out their tasks independently, manage their secure portal for the filing of suspicious transaction reports (STRs), decide which operational or strategic analyses to perform and disseminate information as appropriate (to national or international authorities). Furthermore, they have the power to freeze cash at borders (upon indication and apprehension by the customs administration, ADA) for up to three months, and to freeze funds upon suspicions (for instance, as those received via STRs or cooperation with other FIUs) for an unlimited period of time[573]. They have direct and indirect access to a wide range of databases and have significant IT capabilities (including a secure channel for STR filing and various analytical tools).

As per the 2004 AML/CFT law, all professionals, their directors and employees have the obligation to report suspicious transactions, including attempted suspicious transactions, regardless of the amount of the transaction, to the CRF. Furthermore, legal provisions in place provide that all supervisors, professionals and self-regulatory bodies are allowed to report suspicions to and share information with the CRF, without professional secrecy obligations applying and with identity protection. The number of STRs submitted to the CRF has increased rapidly in recent years, from around7 000 in 2014 to roughly50 000 in 2019, as shown in the figure below. Lastly, the CRF regularly meets with national supervisors and SRBs to exchange feedback on the number and quality of STRs and support in awareness-raising and training sessions. It integrates the Egmont Group and participates in multiple international fora.

Figure 16: CRF – Breakdown of suspicious transaction reports (STRs) received – 2014–2019[574]



[572] Companies can request their data not to be accessible to the general public under certain circumstances – see below

[573] The Law of 10 August 2018 extended CRF's freezing powers, making the validity period of a freezing is no longer limited in time. Before the validity period was limited to 6 months

[574] CRF rapports d'activité 2014-19.

While the **Administration des Contributions Directes (ACD)**, Luxembourg's direct tax administration (e.g. income tax), is not an AML/CFT competent authority, it plays an important role in supporting the detection efforts. The ACD has relevant tax review processes in place and information sharing that contributes to reduce the likelihood of tax crimes and increase the probability of detection should these occur.

Prosecution authorities conduct all necessary actions to investigate and prosecute criminal offenses and recover crime-related assets. The General State Prosecutor *("Procureur général d'Etat")* represents the prosecution authorities in person or through his or her deputies before the Court of Cassation and the Court of Appeal. The state prosecutors represent in person or through their substitutes the prosecution authorities before the District Courts and the Police Courts. The State Prosecutor receives complaints and denunciations (including dissemination reports from the CRF) and assesses the action to be taken on them. He or she takes or causes to be taken all necessary steps to ascertain the truth and to prosecute violations of criminal law. The State Prosecutor supervises to this end the activities of the judicial police in preliminary investigations and may transfer the case to an Investigative Judge to conduct a judicial inquiry if coercive measures are required or if the offence is a crime that cannot be decriminalised (based on a "requisition").

Investigative judges are not part of the prosecution authorities and, as such, remain independent. (nvestigative judges may order measures that restrict individual freedoms (i.e. coercive measures) such as provisional detention, searches and seizures. The **judicial police** 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. Investigative judges have the means to access or request relevant information within inquiries, including to the financial sector.

The powers of Investigative Judges, when providing major mutual legal assistance, and State Prosecutors, when providing ancillary mutual legal assistance, are identical for both domestic and foreign cases. In fact, given Luxembourg's open economy and significant share of international funds, a considerable part of their activities relates to mutual legal assistance (MLA) and other forms of international cooperation (such as among asset recovery offices). ML and TF are both 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 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.

Since the previous mutual evaluation, the number of investigations, prosecutions and convictions for ML/TF has significantly increased. In 2019, the public prosecutor's offices prosecuted 321 persons for ML/TF offenses. In the same year, the courts convicted 355 persons for ML/TF, while 256 judicial investigations for ML/TF were opened. It should be noted that most of the convictions in 2019 relate to prosecutions initiated before 1 January 2019, which is why the number of convictions is higher than the number of prosecutions. The majority of prosecutions related to offences on drug trafficking, robbery or theft, and fraud and forgery, and related to self-laundering cases (i.e. cases where the ML offence is prosecuted on the perpetrator associated with the offence itself and not stand-alone ML).

Table 30: Persons investigated/prosecuted and convicted for ML/TF (2015–2019)[575]

	2015	2016	2017	2018	2019
ML/TF new notices[576]	1 071	1 006	677	549	653
ML/TF investigation (Investigative judge; information)	475	375	282	290	256
ML/TF prosecutions	324	352	260	291	321
ML/TF convictions[577]	260	267	264	353	355

Recovering proceeds and benefits of domestic and foreign crimes is a priority for Luxembourg. State prosecutors and investigative judges have the power to identify and trace the proceeds, benefits and instrumentalities of a predicate offence during a preliminary investigation or judicial inquiry (but not after conviction). Proceeds, benefits and instrumentalities can be seized or confiscated upon conviction (whereby the perpetrator forgoes ownership over his assets, which are transferred to the state). In the period 2017-2019, ML/TF related seizures totalled approximately €104 million for domestic cases, and around €663 million for foreign cases (i.e. following mutual legal assistance requests (MLA) received); most of these relate to fraud and forgery, corruption and bribery, illicit goods trafficking and participation in organised crime.

Table 31: Summary of ML/TF-related seizures, 2017–2019 (€ million)[578]

	2017	2018	2019	2017–19 (sum)
ML/TF-related seizures				
Domestic cases	1.7	9.5	93.2	104.4
Seizures following an MLA received	22.7	180.8	459.3	662.7

Luxembourg's Asset Recovery Office (ARO)[579] is part of the State Prosecutor's Office at the Luxembourg District Court and is responsible for identifying and tracing assets linked to foreign crimes, facilitating the exchange of information with foreign authorities and advising prosecution authorities, Investigative Judges and Judicial Police on measures to take within investigations of foreign crimes.

Moreover, **the Administration des Douanes et Accises (ADA)**, the customs administration, has the authority to temporarily (up to 24 hours) seize undeclared cash >€10 000 or cash suspected as crime proceeds or instrumentalities (at borders); upon reporting this to the CRF, and upon CRF's instruction, cash can be held seized for up to three months. Luxembourg's Asset Recovery Office (ARO) is part of the judicial authorities and is responsible for identifying and tracing assets linked to foreign crimes, facilitating the exchange of information with foreign authorities, and advising prosecution authorities

[575] General State Prosecutor's Office Statistical Service, data received in April 2020; sum of self-laundering, third-party ML, standalone ML and terrorism & terrorist financing; relates to number of persons, not number of cases

[576] Prosecution authorities receive intelligence on ML/TF from a variety of sources (including Police, CRF, Ministries, AML/CFT competent authorities). This is then recorded as a "new notice" in the "JUCHA" case management system. A Prosecutor may decide not to act upon that intelligence, or might launch a preliminary/judicial investigation, which can lead to court-run legal proceedings, and ultimately convictions.

[577] Convictions are counted as per the year of the conviction (and not per year when the new notice was received)

[578] General State Prosecutor's Office Statistical Service.

[579] Bureau de Recouvrement des Avoirs (BRA); on the basis of Decision 2007/845/JHA, each EU State is to set up or designate a maximum of two Asset Recovery Offices to facilitate the tracing and identification of proceeds of crime and other crime-related property that may become the object of a freezing, seizure or confiscation order made by a competent judicial authority in the course of criminal or civil proceedings.

on measures to take within investigations of foreign crimes. Investigations into financial matters of offences with the aim of asset recovery are typically performed by the Judicial Police Service along the judicial process during the investigation phase.

Finally, **international cooperation is at the centre of Luxembourg's AML/CFT approach** given its open economy and diverse working population. This is ensured at the level of each competent authority (via membership in relevant international groups as well as information sharing mechanisms), law enforcement agencies (police cooperation), prosecution authorities (ancillary legal assistance requests), investigative judges (major legal assistance and EAW), MoJ (extraditions) and exchanges with other asset recovery offices (ARO), as well as national level conventions and bilateral and multi-lateral treaties. Importantly, Luxembourg has ratified/signed the Vienna Convention[580], the Palermo Convention[581], the Terrorist Financing Convention[582], the Merida Convention[583], the Council of Europe Convention on Cybercrime (2001) and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism[584]. In 2017 to 2019, the General State Prosecutor has received approximately 500 MLAs per year (of which around 110 per year were ML-related). In 2019, 39 extradition requests were executed from Luxembourg to another country (and 102 from another country to Luxembourg), 41 assistance requests were received by the Asset Recovery Office, and ~1 000 police-to-police ML/TF related messages were exchanged with foreign counterparts.

[580] UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.

[581] UN Convention against Transnational Organized Crime, 2000 (and the Protocols Thereto).

[582] International Convention for the Suppression of the Financing of Terrorism 1999 – adopted by the General Assembly of the UN in resolution 54/109 of 9 December 1999.

[583] UN Convention against Corruption, 2005

[584] Warsaw Convention - Treaty No. 198 – Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism.

7.2. Criminalisation of predicate offences and ML/TF

Money laundering, related predicate offenses and terrorist financing are criminalised under Luxembourg law. This section describes the criminalisation of these offences.

The offence of money laundering is in essence the act of knowingly facilitating deceit as to the nature, origin, location, disposal, movement or ownership of any kind of asset obtained criminally. The definition of money laundering under current law includes[585,586]:

- Knowingly concealing the nature, origin, ownership, placement or movement of goods linked to a predicate offence
- Knowingly supporting the placement, integration or layering of goods linked to a predicate offence
- Knowingly purchasing, holding or reusing goods linked to a predicate offence

The offence of money laundering requires an underlying predicate offence. Luxembourg case law requires that "*the trial judges, seized of a prosecution for the offence of money laundering, must establish, at least in an implicit but certain manner, the existence of the constituent elements of the 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*"[587]. ML is also punishable when the primary offence has been committed abroad. However, excluding offences for which the law allows proceedings to be brought even if they are not punishable in the State in which they were committed, this offence must be punishable in the state in which it was committed[588]. A list of offenses for which the law allows proceedings to be brought even if they are not punishable in the state in which they were committed is provided for in article 5-1 of the CPP. ML is also punishable when the perpetrator is also the perpetrator of or accomplice in the primary offence.

If committed by a natural person, ML is punished by a prison sentence of one to five years and/or a fine of between €1 250 and €1.25 million. The penalty amounts to 15 to 20 years and/or a fine of between €1 250 and €1.25 million if the perpetrator is involved in the main or ancillary activity of an association or organisation. Other ancillary penalties, i.e. special confiscation, closure of a company

---

[585] *En vertu de l'article 506-1 du Code pénal, l'infraction de blanchiment est définie comme suit […] :*

- *Ceux qui ont sciemment facilité, par tout moyen, la justification mensongère de la nature, de l'origine, de l'emplacement, de la disposition, du mouvement ou de la propriété des biens vises à l'article 31, paragraphe 2, point 1°, formant l'objet ou le produit, direct ou indirect de [liste d'infractions primaires] ou constituant un avantage patrimonial quelconque tiré de l'une ou de plusieurs de ces infractions;*
- *Ceux qui ont sciemment apporté leur concours à une opération de placement, de dissimulation, de déguisement, de transfert ou de conversion des biens vises à l'article 31, paragraphe 2, point 1°, formant l'objet ou le produit, direct ou indirect, des infractions énumérées au point 1) de cet article ou constituant un avantage patrimonial quelconque tiré de l'une ou de plusieurs de ces infractions*
- *Ceux qui ont acquis, détenu ou utilisé des biens vises à l'article 31, paragraphe 2, point 1°, formant l'objet ou le produit, direct ou indirect, des infractions énumérées au point 1) de cet article ou constituant un avantage patrimonial quelconque tiré de l'une ou de plusieurs de ces infractions, sachant, au moment où ils les recevaient, qu'ils provenaient de l'une ou de plusieurs des infractions visées au point 1) ou de la participation à l'une ou plusieurs de ces infractions*

[586] Article 8-1 of the 1973 Drug Trafficking Law defines the money laundering offence with regards to drug trafficking (as defined in Article 8 a. and b. of the same law). The definition of money laundering under this law is quasi-identical to the money laundering definition as per Article 506-1 of the Penal Code

[587] Court of Appeal 3 June 2009, Pas. 34, p.636

[588] *Article 506-3 "Les infractions prévues à l'article 506-1 sont également punissables lorsque l'infraction primaire a été commise à l'étranger. Toutefois, à l'exception des infractions pour lesquelles la loi permet la poursuite même si elles ne sont pas punissables dans l'Etat où elles ont été commises, cette infraction doit être punissable dans l'Etat ou elle a été commise*"

or business, publication or display, at the convicted person's cost, of the conviction or a copy thereof, prohibition to exercise certain professional or social activities, are applicable.

If ML is committed by a legal person, the maximum rate of the fine is increased tenfold. A prison sentence does not apply but other ancillary penalties (i.e. special confiscation, exclusion from bidding for public tenders and concession contracts, winding up) are applicable.

Repeat offenders of money laundering may be sentenced to double the maximum legal penalty.

The list of predicate offences includes, on the one hand, a restrictive enumeration of specific articles of the Penal Code or special laws and, on the other hand, an exhaustive reference to any offence punishable by deprivation of liberty for a minimum of more than six months[589]. Since January 2017, the list includes two tax crimes, aggravated tax fraud[590] and tax swindling[591], while simple tax evasion is sanctioned by the competent tax administration and does not come within the provisions of criminal law. The law has introduced thresholds to distinguish simple tax fraud from aggravated tax fraud and tax swindling. Note that the predicate offense of tax swindling was criminalised back in 1993, while aggravated tax fraud was introduced by the 2017 Tax Reform Law.

Terrorism and terrorist financing offenses provided for in articles 112-1, 135-1 to 135-6, 135-9 and 135-11 to 135-16 of the Penal Code are, on one hand, autonomous offenses and, on the other hand, predicate offenses to ML provided for in article 506-1 of the Penal Code. The scope of terrorism and TF has been broadened many times (in 2010, 2012 and 2015) to include the financing of a terrorist act, the financing of a terrorist individual or group, participation in a terrorist group, active and passive terrorist recruitment, active and passive terrorist training, travel for terrorist purposes, etc. In particular, terrorist financing is captured in Article 135-5, and relates to intentionally providing funds of any nature to commit a terrorist act or finance a terrorist individual or group, directly or indirectly (even if not linked to a specific act).

Anyone who commits a terrorist act as defined in article 135-1 of the Penal Code is punished by a criminal sentence 15 to 20 years. He receives a life sentence if this act led to the death of one or more individuals.

Anyone who, wilfully and knowingly, is an active member of a terrorist group, is punished by a prison sentence of one to eight years and/or a fine of between €2 500 and €12 500, even if he did not intend to commit an offence as part of this group or be involved as a perpetrator or accomplice.

Anyone involved in the preparation or execution of any unlawful activity by a terrorist group, knowing that his involvement would contribute towards the group's objectives, is punished by a prison sentence of one to eight years and/or a fine of between €2 500 and €12 500.

Anyone involved in any decision-making as part of a terrorist group, knowing that his involvement would contribute towards the group's objectives, as described in the previous article, is punished by a criminal sentence of five to ten years and/or a fine of between €12 500 and €25 000.

Any leader of a terrorist group is punished by a criminal sentence of 10 to 15 years and/or a fine of between €25 000 and €50 000.

Anyone who has committed an act of terrorist financing as described in sub-paragraph (1) of article 135-5 (financing of terrorist acts) receives the same sentences as those provided for in the articles referred to in sub-paragraph (2) of article 135-5, following the distinctions made in these articles.

[589] Captured in article 506-1 item 28 of the Penal Code : *"de toute autre infraction punie d'une peine privative de liberté d'un minimum supérieur à 6 mois*"

[590] Within the meaning of Article 396 (5) of the General Tax Law

[591] Within the meaning of Article 396 (6) of the General Tax Law

Anyone who has committed an act of terrorist financing as described in sub-paragraph (3) of article 135-5 (financing of a terrorist individual or group) shall receive the same sentences as those provided for in article 135-2, following the distinctions made therein.

No punishment is imposed on anyone who, before attempting to commit the offences referred to in articles 112-1, 135-1, 135-2, 135-5, 135-6, 135-9 and 135-11 to 135-16 and before any proceedings have begun, informs the authorities of action taken in preparation for the offences referred to in these articles or of the identity of the individuals who took this action.

In the same circumstances, custodial sentences are reduced in the manner and to the extent described in article 52 where, after proceedings have begun, the defendant has named perpetrators whom the authorities had previously been unable to identify.

No punishment shall be imposed on anyone convicted of membership of a terrorist group who, before attempting terrorist acts in the group's name and before any proceedings have begun, informs the authorities of this group's existence and names its lead and deputy commanders.

For a natural repeat offender of terrorism and TF acts the following rules do apply:

Anyone who, after having been convicted of a criminal sentence, commits another crime that carries a prison sentence of five to 10 years may be handed down a prison sentence of 10 to 15 years.

If the crime carries a prison sentence of 10 to 15 years, the perpetrator could receive a prison sentence of 15 to 20 years.

If the crime carries a prison sentence of 15 to 20 years, the perpetrator shall receive a prison sentence of at least 17 years.

Legal persons can also be punished for terrorism and TF. Article 36 of the Penal Code provides, in a general manner, that, in criminal matters, the maximum fine applicable to legal persons is €750 000. Article 37 of the same code provides that the maximum imposed under the provisions of article 36 in quintuples in cases where the legal person is criminally liable for certain offenses including acts of terrorism and TF. That raises the maximum fine for terrorism and TF to €3.75 million.

Convicting a legal person of an offence does not preclude natural persons involved in the offence from being convicted for the same offence.

List of predicate offences to ML in Luxembourg (mapped to FATF crime categories, as used in Threats assessment)[592]

Predicate offence (as per Threats Assessment)	Law(s) defining predicate offence	Relevant article(s) within the law (and actual designation in Luxembourg law)	ML predicate offence (CPP)
Fraud and forgery	Code pénal (CP)	489 to 490 (Banqueroute frauduleuse)	506-1, item 10
		491 to 492 (Abus de confiance)	505-1, item 10
		493 (Abus de faiblesse)	506-1, item 10
		494 (Usure)	506-1, item 10
		495 (Production frauduleuse d'une pièce en justice)	506-1, item 10
		496 (Escroquerie et tentative d'escroquerie)	506-1, item 10
		496-1 to 496-4 (Escroquerie à la subvention)	506-1, item 5
		175 (Contrefaçon de titres représentatifs de droits de propriété, de créances ou de valeurs mobilières autres que des signes monétaires)	506-1, item 28
		179 to 182, 186 (Contrefaçon ou falsification de sceaux, timbres, poinçons, marques)	506-1, item 28
		184, 187, 187-1 (Contrefaçon ou falsification de sceaux, timbres, poinçons, marques)	506-1, item 8
		194 to 197 (Faux en écritures)	506-1, item 28
		208 (Faux certificat commis par un fonctionnaire dans l'exercice de sa fonction ; usage de faux certificat)	506-1, item 28
		211 and 212 (Faux commis dans les dépêches télégraphiques)	506-1, item 28
		215, 216, 221, 223 (Faux témoignage et faux serment)	506-1, item 28
	Loi modifiée du 10 août 1915 concernant les sociétés commerciales (L-10.08.1915)	171-1 (Abus de biens sociaux)	506-1, item 28
		165 (Faux bilans)	506-1, item 28
Tax crimes	Loi générale des impôts (LGI)	§ 396 alinéas (5) and (6) (Fraude fiscale aggravée et escroquerie fiscale en matière d'impôts directs)	506-1, item 25
	Loi du 28 janvier 1948 tendant à assurer la juste et exacte perception des droits d'enregistrement (L-28.01.1948)	29, alinéa 1 and 2 (Fraude fiscale aggravée et escroquerie fiscale en matière de droit d'enregistrement)	506-1, item 26
	Loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée (L-12.02.1979)	80, paragraphe 1er (Fraude fiscale aggravée et escroquerie fiscale en matière de TVA)	506-1, item 27
Drug trafficking	Loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie (L-19.02.1973)	8.1 a) and b)	8-1 L-19.02.1973 [593]

[592] Mapping from CRF 2017 Annual Report, as used in threats assessment.

[593] Article 8-1 of the 1973 Drug Trafficking Law defines the money laundering offence with regards to drug trafficking (as defined in Article 8 a. and b. of the same law). The definition of money laundering under this law is quasi-identical to the money laundering definition as per Article 506-1 of the Penal Code

Predicate offence (as per Threats Assessment)	Law(s) defining predicate offence	Relevant article(s) within the law (and actual designation in Luxembourg law)	ML predicate offence (CPP)
	Loi du 11 janvier 1989 réglant la commercialisation des substances chimique à activité thérapeutique (L-11.01.1989)	5	506-1, item 15
Corruption and bribery	Code pénal (CP)	240 (Détournement de deniers publics)	506-1, item 28
		243 (Concussion à l'aide de violences et menaces)	506-1, item 28
		246 to 253 (Corruption active et passive)	506-1, item 6
Participation in an organised criminal group and racketeering	Code pénal (CP)	322 to 324ter (Association de malfaiteurs et organisation criminelle)	506-1, item 2
Counterfeiting and piracy of products	Loi du 18 avril 2001 sur le droit d'auteur (L-18.01.2001)	82 to 85 (Droits d'auteur)	506-1, item 17
	Code pénal (CP)	191 (Contrefaçon de marques)	506-1, item 8
		309 (Violation du secret d'affaires)	506-1, item 8
Smuggling	Loi générale sur les douanes et accises (LGDA)	220 and 231 (Contrebande)	506-1, item 23
Robberies or theft	Code pénal (CP)	463, 464 (Vol simple, vol domestique)	506-1, item 9
		467 to 469, 471 to 473 (Vol qualifié)	506-1, item 28
Sexual exploitation, including sexual exploitation of children	Code pénal (CP)	372 (Attentat à la pudeur : avec violence ou menaces ; sur enfant de moins de 16 ans)	506-1, item 28
		379 (Exploitation de la prostitution)	506-1, item 3
		379bis (Proxénétisme)	506-1, item 3
		383, 383bis, 383ter, and 384 (Outrages publics aux bonnes mœurs et dispositions particulières pour protéger la jeunesse)	506-1, item 4
Trafficking in human beings and migrant smuggling	Code pénal (CP)	382-1 and 382-2 (Traite des êtres humains)	506-1, item 3
		382-4 and 382-5 (Trafic illicite des migrants)	506-1, item 3
Illicit trafficking in stolen and other goods	Loi du 21 mai 1966 concernant a) les fouilles d'intérêt historique, préhistorique, paléontologique ou autrement scientifique ; b) la sauvegarde du patrimoine culturel mobilier (L-21.05.1966)	10 L-21.05.1966	506-1, item 14
Environmental crimes	Loi modifiée du 19 janvier 2004 concernant protection de la nature et des ressources naturelles (L-19.01.2004)	64	506-1, item 18
	Loi modifiée du 21 juin 1976 relative à la lutte contre la pollution de l'atmosphère (L-21.06.1976)	9	506-1, item 19

Predicate offence (as per Threats Assessment)	Law(s) defining predicate offence	Relevant article(s) within the law (and actual designation in Luxembourg law)	ML predicate offence (CPP)
	Loi modifiée du 10 juin 1999 relative aux établissements classés (L-10.06.1999)	25	506-1, item 20
	Loi du 29 juillet 1993 concernant la protection et la gestion de l'eau (L-29.07.1993)	26	506-1, item 21
	Loi modifiée du 17 juin 1994 relative à la prévention et à la gestion des déchets (L-17.06.1994)	35	506-1, item 22
Insider trading and market manipulation	Loi du 9 mai 2006 relative aux abus de marché (L-09.05.2006), article 32	32 (Abus de marché, délit d'initié)	506-1, item 24
Terrorism and terrorist financing	Code pénal (CP)	135-1 to 135-6, 135-9, 135-11 to 135-13	506-1, item 1
Illicit arms trafficking	Loi modifiée du 15 mars 1983 sur les armes et munitions (L-14.03.1983)	28 L-15.03.1983	506-1, item 7
Kidnapping, illegal restraint and hostage taking	Code pénal (CP)	364 (Enlèvement d'un enfant âgé de moins de 7 ans)	506-1, item 28
		368 à 370 (Enlèvement de mineurs)	506-1, item 3
		436 (Détention illégale et arbitraire de plus d'un mois : sur faux ordre de l'autorité publique, faux costume ; menace de mort)	506-1, item 28
		442-1 (Prise d'otages)	506-1, item 28
Extortion	Code pénal (CP)	470 (Extorsion)	506-1, item 28
Counterfeiting currency	Code pénal (CP)	162, 168, 173, 176 and 177 (Fausse monnaie)	506-1, item 28
Murder, grievous bodily injury	Code pénal (CP)	112-1 (Attentat contre les personnes jouissant d'une protection internationale)	506-1, item 1
		136bis to 136 quinquies (Violations graves du droit humanitaire international)	506-1, item 28
		260-1 to 260-3 (Torture)	506-1, item 28
		348 to 350 (Avortement)	506-1, item 28
		375 to 378 (Viol)	506-1, item 28
		393 to 397 (Meurtre, assassinat, parricide, infanticide, empoisonnement)	506-1, item 28
		400 to 401 (Coups et blessures volontaires : maladie incurable ; incapacité permanente ; perte organe ; mutilation ; mort)	506-1, item 28
		401bis (Coups et blessures volontaires sur enfant moins 14 ans accomplis)	506-1, item 28
		403 to 404 (Empoisonnement : maladie incurable ; incapacité permanente ; perte organe ; mort)	506-1, item 28
		407 and 408 (Entrave à convoi ferroviaire : maladie ; incapacité de travail ; maladie incurable ; incapacité permanente ; perte organe ; mutilation grave)	506-1, item 28
		409 paragraphes 2 to 5 (Coups et blessures sur conjoint : préméditation ; maladie ; incapacité temporaire ; maladie incurable ; incapacité permanente ; perte organe ; mutilation grave ; mort)	506-1, item 28

Predicate offence (as per Threats Assessment)	Law(s) defining predicate offence	Relevant article(s) within the law (and actual designation in Luxembourg law)	ML predicate offence (CPP)
		438 (Séquestration illégale-torture-maladie incurable-mort)	506-1, item 28
		474 to 475 (Vol commis à l'aide de violences et menaces : mort ; meurtre commis pour faciliter le vol ou l'extorsion ou pour en assurer l'impunité)	506-1, item 28
		530 to 532 (Destruction volontaire d'objets mobiliers d'autrui : violences ou menaces ; maladie ; lésion corporelle ; meurtre)	506-1, item 28
Piracy	Loi du 14 avril 1992 instituant un code disciplinaire et pénal pour la marine (L-14.04.1992)	64	506-1, item 28
Cybercrime	Code pénal (CP)	509-1 à 509-7 (Certaines infractions en matière informatique)	506-1, item11
	Loi du 14 août 2000 relative au commerce électronique (L-14.08.2000)	48 (Spam)	506-1, item 12

8. EMERGING RISKS, EVOLVING RISKS AND CHALLENGES

In this section, the NRA focuses on the main emerging and evolving risks that Luxembourg is likely to be increasingly exposed to in the future and that will require coordination, supervisory, detection and prosecution authorities to monitor and prepare for going forward. These relate to emerging, evolving and/or unforeseen risks with some impact at present in Luxembourg, but with a future impact that is not fully known, growing or rapidly evolving.

Key emerging and evolving vulnerabilities include VASPs, new payment methods and entities moving from the UK to Luxembourg in the context of Brexit. Key emerging and evolving threats include cybercrime and online extortion. There are also significant developments in advancing technologies applied to AML/CFT mitigating controls, which in turn give rise to dynamic ML/TF risk. An overview is provided below.

8.1. Emerging and evolving vulnerabilities

8.1.1. Virtual assets (VAs) and virtual assets service providers ("VASPs")

At the international level, the global virtual assets (VAs) and virtual asset service providers (VASPs) space has expanded rapidly over the past five years. The increased number of VA and VASP types has been accompanied by an increased volume of VA users, transactions and revenues. The number of VAs users increased from 45 million in 2016 to at least 139 million by 2019[594]. The VASP industry servicing VA users has also expanded rapidly, with VA exchanges generating multi-billion revenues in 2019[595].

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[596]. Furthermore, Luxembourg's domestic market offers a certain level of demand for VA related services. According to various surveys, 4-8% out of ~600 000 of Luxembourg residents own VAs[597,598]. Those factors contributed to VA-related activity being present in Luxembourg. It would include VASPs, such as centralised exchanges, and non-VASP firms developing technologies that are related to VAs. Since the adoption of the 2020 AML/CFT Law, several entities have applied for a VASP registration. As of August 2020, no entity has been registered yet in Luxembourg for such activities. Given the high adoption rate of VAs and new technologies in Luxembourg, there exists also a risk of VASPs established in other jurisdictions but providing services in Luxembourg and thus requiring to be registered in Luxembourg being abused or misused for ML/TF purposes.

Increased user adoption of VAs and their inherent technological features has led to a significant uptake of VAs for ML/TF activities. As described in the "Cross-cutting vulnerabilities" section on virtual assets, VAs may be abused/misused by criminals to power illegal products, marketplaces and investment

[594] Cambridge Centre for Alternative Finance, 2nd Global Cryptoasset Benchmarking Study, December 2018
[595] Messary Crypto, Estimating "Real 10" Exchange Revenue, 11 April 2019
[596] Luxembourg for Finance, https://www.luxembourgforfinance.com/en/financial-centre/fin-tech/
[597] Statista, How many customers own cryptocurrency?, August 2018
[598] TNS Ilres, Le concept des crypto-monnaies au Luxembourg, February 2018

fraud schemes, the combined revenues of which exceeded $1 billion in 2019[599]. VAs are also increasingly used by terrorist financing groups, cybercriminals and sexual exploitation profiteers [600]. Globally, several jurisdictions and international bodies have recognised the rising ML/TF threat of VAs and VASPs. FATF highlighted virtual currencies as one of the key emerging risks to ML and TF, and in particular offences of tax evasion and fraud[601]. The EU Supranational Risk Assessment recognised Vas' and VASPs' rising risk to ML/TF purposes[602]. Further, some countries have explicitly analysed the vulnerability of VAs and VASPs and published correspondent risk assessments, highlighting the threat of VAs being misused or abused for terrorist financing, investor fraud, drug trafficking and other predicate offences.[603] Note that as of July 2020, the Ministry of Justice is in the process of conducting a separate vertical risk assessment on VASPs in close collaboration with the CSSF, the CRF and different Luxembourgish private-sector entities.

In recent months, competent authorities have been setting up mitigating actions to manage the risks of VASPs. Specifically, the CSSF became the dedicated supervisory authority for VASPs for AML/CFT purposes by the 2020 AML/CFT Law of 25 March 2020 and has been granted with powers to take supervisory measures including, among others, conducting off-site supervision and on-site inspections, and imposing sanctions in case of non-compliance with the AML/CTF regulations. On 9 April 2020, the CSSF issued a *"communiqué"* detailing the registration process for VAs established in Luxembourg or providing their services in Luxembourg[604]. While some files are pending approval by the CSSF, at the time of writing of this report, no VASP has been registered yet.

Over past years, the CSSF has also published several general and entity-specific warnings on VASPs and VAs that falsely claim to have a license in Luxembourg. CRF exchanges information with entities functioning in Luxembourg, which report suspicious transactions, and coordinates work with international financial intelligence entities.

Given the rapid expansion in this sector in recent years, and the change in Luxembourg regulatory environment (both described above), it is possible that the number and different types of VASPs established or providing services in Luxembourg will increase. The potentially growing diversity of the VASP landscape will impact associated ML/TF risks and challenges, which should continue to be monitored going forward.

8.1.2. Use of new payment methods

New payment methods (NPMs) are continuously being developed and launched by a variety of players, ranging from emerging innovators (e.g. FinTechs) to traditional entities (e.g. banks or payment/e-money institutions). Both internationally and in Luxembourg, payment preferences are changing to accommodate the need for ease of payment both online and at point of service[605], which in turn has led to an increase in innovative NPMs.

These NPMs can be categorised into those that extend the traditional electronic payment methods (e.g. prepaid cards, internet banking and mobile payments); and those that are not linked to the traditional payment methods on offer (e.g. physical electronic wallet, online and mobile payments

[599] Ciphertrace, Q4 2019 Cryptocurrency Anti-Money Laundering Report, February 2020

[600] Chainalysis, 2020 Crypto Crime Report, January 2020

[601] FATF Report, *Virtual currencies – key definitions and potential AML/CFT risks*, June 2014

[602] European Union Supranational Risk Assessment Update, July 2019

[603] For example: Swiss Interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism (CGMF), *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, 2018

[604] CSSF, *Communiqué on virtual assets, virtual asset service providers and the related registration process* (link)

[605] See, for example: Worldpay, *Global Payments Report*, 2020 (link); and J.P. Morgan, 2019 Global Payments Trends Report – Luxembourg Country Insights, 2019 (link)

that are not directly linked to a bank account, digital precious metals, and virtual currencies). NPMs are available in Luxembourg and allow users to make payments to merchants associated with the network both at the point of sale or online[606], and SEPA cards, a payment-integration initiative of the EU which enables customers to make cashless euro payments from a single payment account under the same conditions as domestic payments, independently of the country of destination within the SEPA-members[607].

There are a number of ML/TF risks that arise in relation to NPMs[608], which include (but are not limited to):

- Exploitation of the non-face-to-face nature of NPM accounts, by both making use of truly anonymised products (i.e. without any customer identification) and by abusing personalised products (i.e. circumventing verification measures by using fake or stolen identities). FATF's recent guidance on digital identity notes that "the growth in digital financial transactions requires a better understanding of how individuals are being identified and verified" and provides guidance on how to apply customer due diligence measures to digital ID systems for verification onboarding and authentication;[609]
- High levels of interaction with third parties. This includes the reliance on third-party funding (including strawmen and nominees) and provision of services with third parties (e.g. card program managers, sellers, retailers) which are often outside the scope of AML/CFT legislation;
- Inability to comply with AML/CFT obligations in relation to recordkeeping, customer screening and reporting requirements either due to cross-border operations or immaturity of the NPM itself may lead to increased abuse for ML/TF purposes; and
- The high negotiability of some NPMs (i.e. that they are widely accepted), ease of transport (i.e. in digital form or via pre-paid card instead of bulk cash) and easy access to cash through ATMs render prepaid cash cards and other NPMs vulnerable to abuse for ML/TF purposes.

As the number and variety of NPMs continues to increase in coming years, entities must assess ML/TF risks before launching an NPM and continue to monitor the ML/TF risks associated with these advances.

8.1.3. Brexit: Entities moving from UK to Luxembourg

The United Kingdom (UK) voted to leave the European Union (EU) in June 2016. The vote was followed by a period of negotiation both between the UK and the EU, and within the UK government to agree the "Withdrawal Agreement". On 31 January 2020, the UK left the EU and entered a transition period that is due to expire at the end of the year. During this period, current rules on trade, travel and business for the UK and EU will apply whilst the UK and EU negotiate additional arrangements, with new rules taking effect on 1 January 2021.

The result of the UK referendum led to a sustained period of political uncertainty, during which several UK-based entities made the decision to relocate the entirety or parts of their business to maintain their link with the single market. Entities across a number of sectors have moved (parts of) their business to Luxembourg, in particular: insurance entities, investment management entities, credit institutions, and alternative asset managers. For example, in 2019, 12 insurance entities relocated from the UK to Luxembourg due to Brexit, increasing the revenues of non-life insurance undertakings by more than double and increasing premia written by life insurance undertakings by more than 15%

[606] https://www.digicash.lu/en/

[607] See, for instance: European Commission (link)

[608] See for instance, FATF, *'Money laundering using new payment methods'* report, 2010 (link)

[609] FATF, *Digital Identity*, 2020 (link)

due to a UK life insurance company transferring a portfolio with a value of approximately €2 billion to Luxembourg.

This growth, however, has not significantly changed the overall ML/TF risk of the affected sub-sectors, as most newcomers offer standardised products and services. Whilst it is expected that the impact of Brexit on Luxembourg is tailing off and that there will be limited further developments, the situation should continue to be closely monitored.

8.2. Emerging and evolving threats

8.2.1. Cybercrime

Cybercrime is considered a significant threat for Luxembourg. While the likelihood is low, given a significant investment in cybersecurity (rendering the country 11th in the world for cybersecurity),[610] potential data breaches can have major consequences on data protection, confidentiality and availability, with important social and economic costs.

Luxembourg's position as a cyber hub increases the likelihood that criminals (in Luxembourg and abroad) commit fraud involving Luxembourg-based institutions and potentially launder the proceeds of that fraud via Luxembourg. Cyber fraud (often coupled with cybercrime) is believed to be increasing[611] and the threat has been strengthened in the context of the global COVID-19 pandemic (see below for further details).

8.2.2. Online extortion

Though few cases of extortion have been reported since 2016, there have been a few significant cases of online extortion in recent years. Online extortion is a crime in which criminals hold data, websites, computer systems or other sensitive information until their demands (e.g. for payment or sexual favours) are met. It may take the form of ransomware or a distributed denial-of-service attack.

According to the Computer Incident Response Centre Luxembourg (CIRCL), a government-driven initiative providing a systematic response facility to computer security threats and incidents, an increasing number of attempted online scams since 2018[612].

Given the increasing reliance on online services for social interaction, information and purchasing of goods both globally and in Luxembourg[613], the threat of online extortion is also likely to increase as criminals continue to develop new ways to exploit the growing pool of potential victims.

8.3. Developments regarding mitigating factors

Regulators and supervised entities have increasingly been seeking technology-enabled solutions to the challenges of effectiveness and efficiency of some long-standing AML/CFT controls (e.g. those

[610] ITU 2019, Global Cybersecurity Index, based on legal, technical, organisation, capacity building and cooperation pillars

[611] Thomson Reuters, *Cybercrime, Financial fraud and money laundering: understanding the new threat landscape*, 2013 (link)

[612] Circl.lu, 2018 (link), Luxembourg Times, 2018 (link)

[613] See, for instance: The Next Web, *Digital trends 2020*, 2020 (link) and DATAREPORTAL, *Digital 2020: Luxembourg,* 2020 (link)

relying on rule-based analysis and manual mechanisms, excessive volumes of false positive alerts in monitoring systems, processing increasing levels of structured data).

Such technologies include blockchain and artificial intelligence and can be used to improve AML/CFT regulatory reporting, risk management, identity management and control, compliance and for transaction monitoring. Some emerging use cases are provided below:

- Customer due diligence: Digital identification and verification technologies in general adopt a two-stage approach: (1) validation of the customer's identity document; and (2) confirmation that the customer is indeed the owner of the document. Advanced technologies enable supervised entities to fulfil their AML/CFT obligations in relation to customer due diligence while improving customer experience;
- Transaction monitoring: Machine learning technologies serve to reduce the large volume of transactions often wrongly identified by rules-based monitoring systems applied by entities and enable human resource to analyse higher value work; and
- Network identification: Applying advanced data-mining techniques to trace and identify networks of transactions and counterparties linked to the customer may enable supervised entities and law enforcement agencies to better identify suspicious activities related to ML/TF.[614]

However, as regulators and supervised entities continue to embrace advanced technology to further strengthen AML/CFT mitigating measures, the vulnerability to several predicate offences may increase the ML/TF risk. For example, criminals may innovate approaches to cybercrime in parallel with the advancements in regulatory technology. Advanced cyberattacks on these systems could impact and/or disable an entities' entire AML/CFT mitigation framework, increasing the risk that ML/TF activity goes undetected, and may at the same time expose the entities themselves to ML/TF threats, such as online extortion.

It is nonetheless expected that regulators and supervised entities will continue to expand their use of advancing technologies to strengthen AML/CFT controls. As adoption of such technology increases, all those engaged must consider and assess the associated ML/TF risks, and plan for appropriate mitigation.

[614] See, for instance: Hong Kong Monetary Authority, *Regtech Watch,* 2020 (link)

9. RESIDUAL RISK ASSESSMENT

The residual risk score is used to identify areas where Luxembourg remains exposed to the highest level of ML/TF risk. It thus serves as a basis to develop and prioritize strategic actions, which can be undertaken to further strengthen Luxembourg's AML/CFT regime and reduce ML/TF risk. The table below provides an overview of the inherent and residual risk by sector assessed in this NRA.

Table 32: Residual risk assessment (at sector-level)

Category	Sector[615]	Inherent risk	Residual risk
Financial sector	Banks	High	Medium
	Investment sector	High	Medium
	Insurance	Medium	Low
	MVTS	High	Medium
	Specialised PFSs	High	Medium
	Market operators	Low	Low
	Support PFSs & other specialised PFSs	Very Low	Very Low
Non-financial sector	Legal professions, chartered accountants, auditors, accountants and tax advisors	High	Medium
	Real estate	High	High
	Freeport operators	High	Medium
	Dealers in goods	Medium	Medium
	Gambling	Low	Low
Legal entities and arrangements		High	High

[615] At the time of writing the NRA, the Ministry of Justice is in the process of conducting a vertical risk assessment on VASPs. These entities became obliged entities only in 2020, with CSSF designated as competent authority for their AML/CFT supervision, and therefore they are not included in the table

10. NATIONAL AML/CFT STRATEGY

Luxembourg is deeply committed to preventing, detecting and prosecuting money laundering (ML) and terrorist financing (TF) activities. Financial crime is a threat to the safety of our society, the integrity of our financial system, and the stability of our economy. Luxembourg has therefore put in place a robust AML/CFT framework to supervise, prevent, gather intelligence on, investigate, prosecute and take all necessary action in the fight against money laundering and terrorist financing activities.

While Luxembourg's national AML/CFT framework is already mitigating effectively a significant part of the ML/TF risks the country is exposed to, we believe that we can further strengthen it to increase effectiveness. The NPC has therefore developed a national AML/CFT strategy, based on the findings of the National Risk Assessment. We defined the national AML/CFT strategy at three levels:

- *Agency-level action plans*: Each competent authority has developed its own action plan to further mitigate the ML/TF risks that its regulated sector is exposed to;
- *National action plan*: We aggregated and articulated these individual action plans into a comprehensive, national plan; and
- *National strategic priorities*: The NPC identified four areas of particular strategic relevance to focus on; those are the areas that the NPC has identified as likely to have the greatest impact on further enhancing the effectiveness of the national AML/CFT framework.

The following paragraphs outline the main strategic priorities.

Further enhancing the prosecution of ML/TF: The NPC will establish a working group consisting of the MoJ, the General State Prosecutor and state prosecutors to identify opportunities to further enhance Luxembourg's approach to prosecuting ML/TF. Specifically, Luxembourg will redefine how the findings of the NRA should feed into the prosecution policy for ML/TF, assess the opportunity to establish a largely autonomous economic and financial crime section at the public prosecutor's office in Luxembourg to deal with these crimes, and increase the level of staffing and expertise.

Further developing the ML/TF investigation capabilities: A working group, consisting of MoJ, MSI, investigative offices and judicial police, will propose an approach to further increase the specialization of investigative judges and judicial police officers for the investigation of economic and financial crime. This may involve setting up a largely autonomous economic and financial crime section within the investigative office in Luxembourg and enhance judicial police teams that are dedicated to these crimes. The working group will also define a recruitment and development strategy for these teams to source and train employees with the skill sets required to investigate complex ML/TF cases.

Harmonising the supervision of DNFBPs: A dedicated working group consisting of MoJ and MoF will review the options to harmonise the governance and capacities of supervisors and the supervisory practices across DNFBPs.

Improving market entry controls of TCSPs: A working group of MoJ, MoF and MoE will make a proposal to define a harmonised authorisation process for TCSP activities across all sub-sectors and review the fit and proper requirements.

Furthermore, the strategy defines a national action plan with seven initiatives that cut across the different elements of Luxembourg's AML/CFT framework. Each of the strategic initiatives includes a set of actions, to be implemented over the course of 2021-2023 by the concerned competent authorities, SRBs, CRF, ARO, prosecution authorities, investigative offices and judicial police. The seven initiatives are:

Initiative I – NPC, MoJ, MoF – Ensure closer collaboration and coordination on a national level: Leverage the existing structure of the NPC Secretariat to further enhance coordination across the national AML/CFT framework and establish closer cooperation, with specific focus on overseeing the implementation of the AML/CFT strategy, further coordinating and streamlining AML/CFT efforts and cooperation, and monitoring changes to the legal framework required.

Initiative II – Supervisory authorities and SRBs - Harmonise the supervisory approach and practices across agencies through closer collaboration and sharing best practices on, among others, the application and enhancement of a risk-based approach and further increasing the effectiveness of supervision and enforcement.

Initiative III – CRF – Further enhance internal capabilities of the financial intelligence unit: Build out the internal capabilities of the CRF, especially, to further enhance the strategic and risk-based approach with additional resources, use of databases and advanced tools and cooperation with supervisors, SRBs and private sector.

Initiative IV – MoJ, MoF, RCS, AED, Supervisory Authorities, SRBs – Increase transparency of legal entities and arrangements: Improve monitoring of data accuracy for legal entities and arrangements (in particular beneficial ownership data), increase awareness of the requirements regarding the use of the beneficial ownership (BO) registers and increase understanding of ML/TF risks regarding legal entities and arrangements.

Initiative V – CI, SPJ, prosecution authorities – Enhance investigation and prosecution organisation, especially the SPJ: Enhance the investigation and prosecution organisation, by implementing new model; increase specialisation of teams and consider using new IT tools, in order to further improve the number of investigations and their translation into legal enforcement; and specifically enhance setup and resources of the SPJ to increase effectiveness of ML/TF investigations.

Initiative VI – ARO – Set up an autonomous and effective asset recovery office: Implement the new model and develop the asset recovery office to a well-equipped and effective agency dedicated to tracing and managing assets.

Initiative VII – Supervisory authorities, SRBs, CRF, ARO, prosecution authorities, CI, SPJ, MoJ, MoF – Continue to monitor and take an active part in international fora and implement changes required: Leverage the existing set up to continue international cooperation, continue to monitor and take part in discussions on an international level, especially in the EU, and implement changes required.

APPENDIX A. METHODOLOGY

A.1. Sectors and sub-sectors – vulnerabilities assessment

Table 33: Sectors and sub-sectors analysed in the vulnerabilities assessment

Sector		Sub-sectors	Supervising agency / department
1	**Banks**	Retail and business banks	CSSF – Banques
		Wholesale, corporate and investment banks	
		Private banking	
		Custodians and sub-custodians (including CSDs)	
2	**Investment sector**	Wealth and asset managers	CSSF – Entreprises d'investissements
		Brokers and broker-dealers (non-banks)	
		Traders/market makers	
		Collective investments	CSSF – OPC
		Regulated securitisation vehicles	
		CSSF-supervised pension funds	
3	**MVTS**[616]	Payment institutions	CSSF – IPIG
		E-money institutions	
		Agents and e-money distributors acting on behalf of PI/EMIs established in other European Member States	
4	**Specialised PFSs**	Specialised PFSs providing corporate services	CSSF – PSF Spécialisés
		Professional depositaries	
5	**Market operators**	Market operators	CSSF – MAF
6	**Support PFSs and other specialised PFSs**	PSF de support	CSSF – Various departments
		Other specialised PFSs	
7	**Insurance**	Life insurers	CAA
		Non-life insurers	
		Reinsurance	
		Intermediaries	
		Professionals of the insurance sector (PSA)	
		CAA-supervised pension funds	
8	**Legal professions, chartered accountants, auditors, accountants, legal advisors and TCSPs**	Lawyers	OAL / OAD
		Notaries	CdN
		Bailiffs *("Huissiers de justice")*	CdH
		(Approved) statutory auditors and (approved) audit firms *("Réviseurs d'entreprises")*	IRE
		Chartered professional accountants *("Experts-comptables")*	OEC

[616] As of the time of writing the NRA, the Ministry of Justice is in the process of conducting a vertical risk assessment on VASPs. These entities became obliged entities only in 2020, with CSSF designated as competent authority for their AML/CFT supervision, and therefore they are not included in the table.

Sector		Sub-sectors	Supervising agency / department
		Accounting professionals and tax advisors	AED
		TCSPs – Administrateurs / directors[617]	
		TCSPs – Business offices[617]	
9	**Real estate activities**	Real estate agents (“agents immobiliers”)	AED
		Real estate developers (“promoteurs immobiliers”)	
10	**Dealers in goods**	Precious metals / jewellers / clocks	AED
		Car dealers	
		Art / Antiques	
		Luxury goods (e.g. maroquinerie)	
11	**Gambling**	Casino	AED[618]
		Sports betting[619]	
		Ad hoc lotteries	
		National lottery	
		Online gambling[620]	
12	**Freeport operators**	Freeport operators	AED
13	**Legal entities and arrangements**	Domestic fiduciaries (“fiducies”)	AED (not supervision, BO registry only)
		Foreign trusts	
		Commercial companies	LBR (not supervision, BO registry only)
		Sociétés civiles	
		Foundations	
		ASBLs	
		Other legal entities	

[617] The scorecards of TCSPs under the AED supervision are combined into one

[618] Although AML/CFT supervision falls under the AED as per the amendment of the law of 13 February 2018 to the 2004 AML/CFT law, some supervisory powers in the gambling sector are held by the Ministry of Justice, the Ministry of Finance, and the Ministry of State, depending on the type of institution.

[619] Analysis covered in NRA text version. No separate scorecard in appendix as activity not present in Luxembourg

[620] Analysis covered in NRA text version. No separate scorecard in appendix as activity not present in Luxembourg

A.2. Threats methodology

Table 34: Predicate offences analysed in the threats assessment

Predicate offences in Luxembourg law	FATF categories[621]
Terrorisme et financement du terrorisme	Terrorism and terrorist financing
Fraude et faux	Fraud and forgery
Trafic illicite de stupéfiants et de substances psychotropes	Illicit trafficking in narcotic drugs and psychotropic substances
Vol	Robbery or theft
Infractions fiscales pénales	Tax crimes
Corruption	Corruption and bribery
Abus de marché	Insider trading and market manipulation
Traite des êtres humains et trafic illicite de migrants	Trafficking in human beings and migrant smuggling
Exploitation sexuelle, y compris celle des enfants	Sexual exploitation, including sexual exploitation of children
Contrefaçon et piratage des produits	Counterfeiting and piracy of products
Participation à un groupe criminel organisé et participation à un racket	Participation in an organised criminal group and racketeering
Contrebande	Smuggling
Trafic illicite de biens volés et autres biens	Illicit trafficking in stolen and other goods
Infractions pénales contre l'environnement	Environmental crimes
Trafic illicite d'armes	Illicit arms trafficking
Extorsion	Extortion
Meurtres et blessures corporelles graves	Murder, grievous bodily injury
Enlèvement, séquestration et prise d'otages	Kidnapping, illegal restraint and hostage taking
Faux monnayage	Counterfeiting currency
Piraterie	Piracy (maritime)
Cybercriminalité	Computer crime

[621] FATF Guidance: National ML/TF Risk Assessment, February 2013, Annex 1

Table 35: Scorecard of criteria for threats

Criteria	Sub-criteria	Example of indicators that can be used	
Probability of crime ("likelihood")	Level of criminality	• Crime rate/number of crimes (domestic) • Terrorist events (incidents, attempts, casualties, etc.) • Presence and activities of known terrorist groups • Number of offences, open/new notices, prosecutions and convictions (with and without ML)	• Assessment is a combination of data and expert opinion, as well as discussion with expert authorities • Data will be collected to support assessment as much as possible – Availability and granularity will differ per crime and criteria (e.g. reputation impacts vs. number of domestic crimes) – Often the relative order of magnitude matters (e.g. corruption index showing Luxembourg as more/less corrupt than others as an indication of internal level) • Flexibility in assessment is needed given crimes' differing nature and materiality – not all will have the same level and granularity of data – not all criteria will be equally relevant to all crimes – Some crimes will merit more time/ data/judgement for assessment vs. others based on materiality, in line with risk-based approach (e.g. maritime piracy in Luxembourg likely immaterial) • Assigning a threat level (low to high) to each crime will thus be based on a mix of information that was possible to collect (data, rankings, indices, surveys, etc.) and expert judgement
Proceeds of crime ("size" and "complexity")	Proceeds generated	• Amounts seized • Estimated value generated per crime committed • Estimate of trade and financial flows with foreign countries (in particular with high risk countries) • Estimated value of proceeds from international crimes • Number of STRs and SARs filed	
	Form of proceeds	• Cash proceeds vs. non-cash physical • Use of innovative forms (e.g. virtual currencies)	
	ML expertise	• Sophistication (knowledge, skills, expertise) • Capability (network, resources, etc.)	
	Geography	• Origin/source • Destination	
Human, social and reputational impact ("consequences")	Economic and social cost	• Foregone revenues • Financial system stability and its perceived integrity • Attractiveness of the country for business, ability to attract FDI, broad "reputation" of country	
	Human harm	• Direct harm to people (injuries, fatalities) • Social harm (e.g. fear of terror, reduced social cohesion)	

A.3. Vulnerabilities methodology

Table 36: Scorecard of assessment criteria for sectorial vulnerabilities

Dimension	Sub-dimension	Examples of indicators/data
Structure	Size	• Revenue/turnover and profit • Assets • Assets under management
	Fragmentation/complexity	• Number of institutions • Level of concentration (e.g. top five entity assets as a % of the market)
Ownership/ legal structure	Ownership/ legal structure	• % ownership by foreign BOs (of which from risky countries based on FATF lists) • % of entities with foreign mother
Products/ activities	Products/activities	• % of high-risk products (e.g. % revenue from products/activities)
Geography	International business	• % of international business (e.g. in clients revenue, assets, transactions)
	Flows with weak AML CFT measures geographies	• % of high-risk geographies based on FATF list of geographies with weak AML/CFT measures (e.g. in clients revenue, assets, transactions)
Clients/ transactions	Volume	• Number of clients • Total number (stock) • New clients per year (flow)
	Risk	• % high-risk clients (based on supervised entities' internal models) • % PEPs (over time): domestic vs. foreign
Channels	Channels	• Type of interaction: % face-to-face, indirect (e.g. online), via intermediaries
Typical ML/TF methods	Threats exposure	• Number of cases of predicate offences using this (sub-) sector
	ML/TF methods observed in Lux	• Number of cases identified (e.g. STRs, convictions, examinations) • Luxembourg expert knowledge (e.g. case studies)
	Sector-specific ML/TF methods	• FATF guidance • Egmont Group case studies • Other countries (e.g. case studies, NRAs)

Used as a corroborating factor

Table 37: Inherent risk scorecard – individual risk ratings

Risk rating against criteria	Risk levels
1	Very Low
2	Low
3	Medium
4	High
5	Very High

Table 38: Inherent risk scorecard risk – overall inherent risk outcome

Average between		
Lower bound	**Higher bound**	**Risk levels**
1.00	1.80	Very Low
1.80	2.60	Low
2.60	3.40	Medium
3.40	4.20	High
4.20	5.00	Very High

A.4. Mitigating factors and residual risk approach

Table 39: Scorecard of impact criteria for mitigating factors

Dimension	Criteria	Information/data used (examples)
Market entry controls	Market entry	• Licenses/registrations – number of applications received, processed, approved, rejected
	Breaches	• Number of licenses/registrations breaches identified / remediated
Understanding of ML/TF risks and AML/CFT obligations	Understanding of ML/TF risks and AML/CFT obligations	• Annual questionnaires • Risk assessments (e.g. entity level, sub-sector risk assessments) • Internal trainings • Supervisors' publications on ML/TF risks in the sector
	Regulation & information	• Type of supervisor (e.g. association, ministry, dedicated supervisor) • Regulation communication to the sector (e.g. circulars) • Education to private sector (e.g. publications, trainings, etc.)
Prevention / Private sector controls	ML/TF controls in place	• CDD / KYC approach, aligned with risk level, number of customers declined based on CDD • Transaction monitoring approach, aligned with risk level, number of alerts generated, handled and STRs reported
	Internal supporting structures	• Formalised policies, procedures and controls, clearly articulating the risk-based AML/CFT approach • Member of management body responsible for compliance with AML/CFT obligations
Supervision & enforcement	Level of supervision	• Number and type of inspections (on-sites and off-sites) • Supervisor procedures formalised and up to date
	Enforcement	• Remedial actions imposed (i.e. number of sanctions and other actions) • Outcomes of remedial actions (i.e. number of deficiencies remediates)
Detection, Prosecution & asset recovery	STRs/SARs	• Number of STRs and SARs issued by subsector and predicate offences • Quality of STRs and SARs issued by subsector and predicate offences
	FIU analyses	• Number of FIU analyses by subsector and predicate offence
	Investigations / prosecution / convictions	• Number of investigations/prosecutions/convictions against subsector entities by subsector and predicate offence
	Seizures / confiscations	• Number of seizures/confiscations and total value by subsector and predicate offence

Figure 17: Residual risk calculation

Inherent risk scorecard risk – overall inherent risk outcome

Inherent risk (i.e. in the absence of controls)

Avg. between Lower bound	Higher bound	Risk levels
1.00	1.80	Very Low
1.80	2.60	Low
2.60	3.40	Medium
3.40	4.20	High
4.20	5.00	Very High

—

—

Mitigating factors scorecard – overall impact on residual risk outcome

Mitigating factors

Avg. between Lower bound	Higher bound	**Outcome** (mitigating factors in place)	Impact on residual risk
1.00	1.80	Limited or no mitigating factors	0
1.80	2.60	Some mitigating factors	-0.5
2.60	3.40	Significant mitigating factors	-1
3.40	4.20	High mitigating factors	-1.5
4.20	5.00	Very high mitigating factors	-2

=

=

Residual risk

Same as inherent risk scores

As an example, a given sub-sector "X" could have:

- Inherent risk score of 3.8 (average across the inherent risk criteria). This corresponds to a level of "High" inherent risk;
- Mitigating factors score: 2.1 (average across the residual risk criteria). This corresponds to an outcome of "some mitigating factors in place" and hence to a reduction of inherent risk by -0.5.
- Residual risk score: 3.8-0.5 = 3.3, which corresponds to a residual risk outcome of "Medium".

These residual risks outcomes are presented in the residual risk assessment section further below.

APPENDIX B. LIST OF FIGURES AND TABLES

B.1. List of figures

B.2. List of tables

B.3. List of case studies

APPENDIX C. DEFINITIONS AND GLOSSARY

C.1. Glossary of laws

Note that most laws in the table below have been modified / amended by following laws. This document always refers to the laws as modified by following laws, up until 30/6/2020. The description under 'term' is the description used to refer to this law in the NRA.

Term	Definition
1915 Companies Law	Loi du 10 août 1915 concernant les sociétés commerciales
1928 NPOs Law	Loi du 21 avril 1928 sur les associations et les fondations sans but lucratif
1931 General Tax Law	Abgabenordnung vom 22. Mai 1931 (Loi générale des impôts du 22 mai 1931)
1948 Registration and Succession Tax Law	Loi du 28 janvier 1948 tendant à assurer la juste et exacte perception des droits d'enregistrement et de succession
1965 Benelux Treaty Law	Loi du 26 février 1965 portant approbation: 1. du Traité d'extradition et d'entraide judiciaire en matière pénale entre le Royaume de Belgique, le Grand-Duché de Luxembourg et le Royaume des Pays-Bas; 2. du Protocole concernant la responsabilité civile pour les agents en mission sur le territoire d'une autre Partie, signés à Bruxelles, le 27 juin 1962
1967 Income Tax Law	Loi du 4 décembre 1967 concernant l'impôt sur le revenu
1973 Drug Trafficking Law	Loi du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie
1976 Strasbourg Convention Law	Loi du 21 juillet 1976 portant approbation de la Convention européenne d'entraide judiciaire en matière pénale, signée à Strasbourg, le 20 avril 1959
1976 Notaries Law	Loi du 9 décembre 1976 relative à l'organisation du notariat
1977 Gambling Law	Loi du 20 avril 1977 relative à l'exploitation des jeux de hasard et des paris relatifs aux épreuves sportives
1979 VAT Law	Loi du 12 février 1979 concernant la taxe sur la valeur ajoutée
1979 Casino Gambling Regulation	Règlement grand-ducal du 12 février 1979 pris en exécution des articles 6 et 12 de la loi du 20 avril 1977 relative à l´exploitation des jeux de hasard et des paris relatifs aux épreuves sportives
1980 Judiciary Organisation Law	Loi du 7 mars 1980 sur l'organisation du judicaire
1987 Sports Betting Regulation	Règlement grand-ducal du 7 septembre 1987 concernant les paris relatifs aux épreuves sportives
1990 Bailiff Law	Loi du 4 décembre 1990 portant organisation du service des huissiers
1991 Lawyers Law	Loi du 10 août 1991 sur la profession d'avocat
1991 Insurance Law	Loi du 6 décembre 1991 sur le secteur des assurances.
1992 Vienna Convention Law	Loi du 17 mars 1992 portant 1. approbation de la Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes, faite à Vienne, le 20 décembre 1988; 2. modifiant et complétant la loi du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie; 3. modifiant et complétant certaines dispositions du Code d'instruction criminelle
1993 LSF Law[622]	Loi du 5 avril 1993 relative au secteur financier
1993 ADA Law	Loi du 27 juillet 1993 portant organisation de l'administration des douanes et accises
1998 CSSF Law	Loi du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier

[622] Sometimes just referred to as "LSF Law" or "LSF"

Term	Definition
1999 Police Law	Loi du 31 mai 1999 portant création d'un corps de police grand-ducale et d'une inspection générale de la Police
1999 Domiciliation Law	Loi du 31 mai 1999 régissant la domiciliation des sociétés
1999 CPAs Law	Loi du 10 juin 1999 portant organisation de la profession d'expert-comptable
2000 MLA Law	Loi du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale
2001 Strasbourg Convention Law	Loi du 14 juin 2001 portant 1. approbation de la convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime, faite à Strasbourg, le 8 novembre 1990; 2. modification de certaines dispositions du code pénal. 3. modification de la loi du 17 mars 1992 1. portant approbation de la Convention des Nations-Unies contre le trafic illicite de stupéfiants et de substances psychotropes, faite à Vienne, le 20 décembre 1988; 2. modifiant et complétant la loi du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie; 3. modifiant et complétant certaines dispositions du code d'instruction criminelle.
2001 Extradition Law	Loi du 20 juin 2001 sur l'extradition
2002 Data Protection Law	Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.
2002 RCS Law	Loi du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises et modifiant certaines autres dispositions légales
2003 Fiducies and Trusts Law	Loi du 27 juillet 2003 - portant approbation de la Convention de La Haye du 1er juillet 1985 relative à la loi applicable au trust et à sa reconnaissance; - portant nouvelle réglementation des contrats fiduciaires, et - modifiant la loi du 25 septembre 1905 sur la transcription des droits réels immobiliers
2003 Terrorism Law	Loi du 12 août 2003 portant 1) répression du terrorisme et de son financement 2) approbation de la Convention internationale pour la répression du financement du terrorisme, ouverte à la signature à New York en date du 10 janvier 2000
2004 AML/CFT Law	Loi du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme
2004 EAW Law[623]	Loi du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union européenne
2004 Securitisation Law	Loi du 22 mars 2004 relative à la titrisation
2004 SICAR Law	Loi du 15 juin 2004 relative à la Société d'investissement en capital à risque (SICAR)
2005 Pension Funds Law	Loi du 13 juillet 2005 relative aux institutions de retraite professionnelle sous forme de société d'épargne-pension à capital variable (sepcav) et d'association d'épargne-pension (assep)
2007 SIF Law	Loi du 13 février 2007 relative aux fonds d'investissement spécialisés
2008 Tax Authorities Cooperation Law	Loi du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines et de l'Administration des douanes et accises
2009 Lottery Law	Loi du 22 mai 2009 relative à l'Oeuvre Nationale de Secours Grande-Duchesse Charlotte et à la Loterie Nationale et modifiant: - la loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu; - la loi modifiée du 20 avril 1977 relative à l'exploitation des jeux de hasard et des paris relatifs aux épreuves sportives

[623] EAW: European Arrest Warrant

Term	Definition
2009 Database Law	Loi du 5 juin 2009 relative à l'accès des autorités judiciaires, de la Police et de l'Inspection générale de la Police à certains traitements de données à caractère personnel mis en oeuvre par des personnes morales de droit public
2009 PSL	Loi du 10 novembre 2009 relative aux services de paiement, à l'activité d'établissement de monnaie électronique et au caractère définitif du règlement dans les systèmes de paiement et les systèmes de règlement des opérations sur titres
2010 Tax Information Exchange Law	Loi du 31 mars 2010 portant approbation des conventions fiscales et prévoyant la procédure y applicable en matière d'échange de renseignements sur demande
2010 AML/CFT Law	Loi du 27 octobre 2010 portant renforcement du cadre légal en matière de lutte contre le blanchiment et contre le financement du terrorisme
2010 Cash Control Law	Loi du 27 octobre 2010 portant organisation des contrôles du transport physique de l'argent liquide entrant au, transitant par le ou sortant du Grand-Duché de Luxembourg
2010 MLA Law	Loi du 27 octobre 2010 portant 1. approbation de la Convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne 2. approbation du Protocole du 16 octobre 2001 à la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne 3. modification de certaines dispositions du Code d'instruction criminelle et de la loi du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale
2010 OPC Law	Loi du 17 décembre 2010 concernant les organismes de placement collectif
2011 Corruption Law	Loi du 13 février 2011 renforçant les moyens de lutte contre la corruption
2012 Family Office Law	Loi du 21 décembre 2012 relative à l'activité de Family Office et portant modification de: - la loi modifiée du 5 avril 1993 relative au secteur financier, - la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme
2012 Terrorism Law	Loi du 26 décembre 2012 portant approbation de la Convention du Conseil de l'Europe sur la prévention du terrorisme, signée à Varsovie, le 16 mai 2005, et modifiant - le Code pénal; - le Code d'instruction criminelle; - la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne; - la loi modifiée du 11 avril 1985 portant approbation de la Convention sur la protection physique des matières nucléaires, ouverte à la signature à Vienne et à New York en date du 3 mars 1980; et - la loi modifiée du 14 avril 1992 instituant un code disciplinaire et pénal pour la marine.
2013 AIFM Law	Loi du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs
2013 Tax Law	Loi du 29 mars 2013 transposant la directive 2011/16/UE du Conseil du 15 février 2011 relative à la coopération administrative dans le domaine fiscal et abrogeant la directive 77/799/CEE et portant 1. modification de la loi générale des impôts ; 2. abrogation de la loi modifiée du 15 mars 1979 concernant l'assistance administrative internationale en matière d'impôts directs
2013 PSA law	Loi du 12 juillet 2013 portant modification de: - la loi modifiée du 6 décembre 1991 sur le secteur des assurances ; - la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme
2015 Free Zone Operator Law	Loi du 24 juillet 2015 modifiant: - la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée; - la loi modifiée du 17 décembre 2010 fixant les droits d'accise et les taxes assimilées sur les produits énergétiques, l'électricité, les produits de tabacs manufacturés, l'alcool et les boissons alcooliques; - la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme.
2015 Tax Law	Loi du 24 juillet 2015 portant approbation 1. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des Etats-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et relatif aux dispositions des Etats-Unis d'Amérique concernant l'échange d'informations communément appelées le «Foreign Account Tax Compliance Act », y compris ses deux annexes ainsi que le

Term	Definition
	«Memorandum of Understanding» y relatif, signés à Luxembourg le 28 mars 2014 2. de l'échange de notes y relatives, signées les 31 mars et 1er avril 2015
2015 Insurance Law	Loi du 7 décembre 2015 sur le secteur des assurances
2015 CRS Law	Loi du 18 décembre 2015 concernant l'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale et portant 1. transposition de la directive 2014/107/UE du Conseil du 9 décembre 2014 modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal; 2. modification de la loi modifiée du 29 mars 2013 relative à la coopération administrative dans le domaine fiscal
2016 Audit profession Law	Law of 23 July 2016 concerning the audit profession and: - transposing Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts; - implementing Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC; - amending the Law of 13 July 2005 on institutions for occupational retirement provision in the form of a SEPCAV and an ASSEP, as amended; - amending the Law of 10 August 1915 on commercial companies, as amended; - repealing the Law of 18 December 2009 concerning the audit profession
2016 SRE Law	Loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État
2016 Tax Law	Loi du 23 décembre 2016 portant transposition de la directive (UE) 2016/881 du Conseil du 25 mai 2016 modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal et concernant les règles de déclaration pays par pays pour les groupes d'entreprises multinationales
2017 Tax Reform Law	Loi du 23 décembre 2016 portant mise en oeuvre de la réforme fiscale 2017
3AMLD	Directive EU 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing
4AMLD	Directive (EU) 2015/849 of the European Parliament and the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC
Code of Criminal Procedure (or CPP)	Code de procédure pénale
Penal Code	Code pénal
13 February 2018 AML/CFT Law	Loi du 13 février 2018 portant 1. transposition des dispositions ayant trait aux obligations professionnelles et aux pouvoirs des autorités de contrôle en matière de lutte contre le blanchiment et contre le financement du terrorisme de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission ; 2. mise en œuvre du règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006 ; 3. modification de : a) la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ; b) la loi modifiée du 10 novembre 2009 relative aux services de paiement ; c) la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat ; d) la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice ; e) la loi modifiée du 10 août 1991 sur la profession d'avocat ; f) la loi modifiée du 5 avril 1993 relative au secteur financier ; g) la loi modifiée du 10 juin 1999 portant organisation

Term	Definition
	de la profession d'expert-comptable ; h) la loi du 21 décembre 2012 relative à l'activité de Family Office ; i) la loi modifiée du 7 décembre 2015 sur le secteur des assurances ; j) la loi du 23 juillet 2016 relative à la profession de l'audit
2018 Police Exchange of Information Law	Loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière et portant : 1) transposition de la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne ; 2) mise en œuvre de certaines dispositions de la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière
2018 Police Reform Law	Loi du 18 juillet 2018 sur la Police grand-ducale et portant modification : 1°du Code de procédure pénale ; 2°de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État ; 3°de la loi du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 4°de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 5°de la loi du 18 décembre 2015 relative à l'accueil des demandeurs de protection internationale et de protection temporaire, et modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat ; et portant abrogation : 1°de la loi du 29 mai 1992 relative au Service de Police Judiciaire et modifiant 1. la loi modifiée du 23 juillet 1952 concernant l'organisation militaire ; 2. le code d'instruction criminelle ; 3. la loi du 16 avril 1979 ayant pour objet la discipline dans la Force publique ; 2°de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police
2018 Payment Services Law	Loi du 20 juillet 2018 portant : 1° transposition de la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/ CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/ CE ; et 2° modification de la loi modifiée du 10 novembre 2009 relative aux services de paiement
2018 AML Information Law	Loi du 1er août 2018 portant transposition de la directive (UE) 2016/2258 du Conseil du 6 décembre 2016 modifiant la directive 2011/16/UE en ce qui concerne l'accès des autorités fiscales aux informations relatives à la lutte contre le blanchiment de capitaux et modifiant 1. la loi modifiée du 29 mars 2013 relative à la coopération administrative dans le domaine fiscal ; 2. la loi du 18 décembre 2015 relative à la Norme commune de déclaration (NCD), et 3. la loi du 23 décembre 2016 relative à la déclaration pays par pays
2018 Asset Confiscation Law	Loi du 1er août 2018 portant modification 1° du Code pénal ; 2° du Code de procédure pénale ; 3° du Nouveau Code de procédure civile ; 4° de la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne ; 5° de la loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie ; 6° de la loi modifiée du 10 août 1991 sur la profession d'avocat ; 7° de la loi modifiée du 17 mars 1992 portant 1. approbation de la Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes, faite à Vienne, le 20 décembre 1988 ; 2. modifiant et complétant la loi du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie ; 3. modifiant et complétant certaines dispositions du Code d'instruction criminelle ; 8° de la loi modifiée du 14 juin 2001 portant 1. approbation de la Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime, faite à Strasbourg, le 8 novembre 1990 ; 2. modification de certaines dispositions du code pénal ; 3. modification de la loi du 17 mars 1992 1. portant approbation de la Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes, faite à Vienne, le 20 décembre 1988 ; 2. modifiant et complétant la loi du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie ; 3. modifiant et complétant certaines dispositions du Code d'instruction criminelle, en vue d'adapter le régime de confiscation

Term	Definition
2018 Criminal Data Protection Law	Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale
2018 EIO Law	Loi du 1er août 2018 portant 1° transposition de la directive 2014/41/UE du Parlement européen et du conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale ; 2° modification du Code de procédure pénale ; 3° modification de la loi modifiée du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale
2018 AED Organisation Law	Loi du 10 août 2018 portant organisation de l'Administration de l'enregistrement, des domaines et de la TVA
2018 FIU Law	Loi du 10 août 2018 modifiant : 1° le Code de procédure pénale ; 2° la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ; 3° la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ; 4° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État afin de porter organisation de la Cellule de renseignement financier (CRF)
2018 Fiducies Information Law	Loi du 10 août 2018 relative aux informations à obtenir et à conserver par les fiduciaires et portant transposition de l'article 31 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission
2018 IDD Law	Loi du 10 août 2018 portant transposition de la directive (UE) 2016/97 du Parlement européen et du Conseil du 20 janvier 2016 sur la distribution d'assurances et modifiant la loi modifiée du 7 décembre 2015 sur le secteur des assurances
2019 RBE Law	Loi du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs et portant 1° transposition des dispositions de l'article 30 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission ; 2° modification de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises
2019 Network and Information System Security Law	Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale
2020 Terrorism Law	Loi du 3 mars 2020 modifiant : 1° le Code pénal ; 2° le Code de procédure pénale, aux fins de transposition de la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil
2020 AML/CFT Law	Loi du 25 mars 2020 portant modification de: 1° la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme; 2° la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat ; 3° la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice ; 4° la loi modifiée du 10 août 1991 sur la profession d'avocat ; 5° la loi modifiée du 10 juin 1999 portant organisation de la profession d'expert-comptable ; 6° la loi modifiée du 23 juillet 2016 relative à la profession de l'audit,

Term	Definition
	en vue de la transposition de certaines dispositions de la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE.
2020 RBASD Law	Loi du 25 mars 2020 instituant un système électronique central de recherche de données concernant des comptes de paiement et des comptes bancaires identifiés par un numéro IBAN et des coffres-forts tenus par des établissements de crédit
2020 RFT Law	Loi du 10 juillet 2020 portant transposition de l'article 31 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, tel que modifié par la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE

C.2. Glossary of key terms and definitions

Term	Definition
ABBL	Association des Banques et Banquiers Luxembourg – Luxembourg Banker's Association
ACD	Administration des Contributions Directes – Direct tax administration
ADA	Administration des douanes et accises – Customs and Excise Administration
AED	Administration de l'Enregistrement et des Domaines et de la TVA
AEOI	Automatic exchange of information
AFU	Anti-Fraud Unit – AED's Service Anti-Fraude
AIF	Fonds d'investissement alternative – Alternative Investment Fund
AIFM	Gestionnaire de fonds d'investissement alternatif – Alternative Investment Fund Manager
Agencies	Public and private-sector institutions part of the AML/CFT institutional framework; used interchangeably with "competent authority"
ALCO	Association Luxembourgeoise des Compliance Officers - Luxembourg Association of Compliance Officers
ALFI	Association luxembourgeoise des fonds d'investissement - Association of the Luxembourg Fund Industry
AML	Anti-money laundering
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism (or Lutte contre le Blanchiment de Capitaux/Financement du Terrorisme (LBC/FT))
AML/CFT supervisors	Supervisory authorities (incl. CSSF, CAA, AED) and SRBs
AuM	Assets under Management
ARO	Luxembourg's Asset Recovery Office (the Bureau de Recouvrement des Avoirs – BRA)
ASBL	Associations sans but lucratif (non-profit organisations)
Auto-saisine	Act of an authority without formal prompting from another party (i.e. *sua sponte*). In the context of this document: decision by a magistrate to initiate an investigation of its own accord
BCL	Banque Centrale du Luxembourg – Central Bank of Luxembourg
BN	Billion

BO	Beneficial Owner (or Bénéficiaire effectif)
CAA	Commissariat aux Assurances – Insurance Supervisory Authority of Luxembourg
CDD	Customer due diligence
CdH	Chambre des Huissiers de justice (Self-regulatory body of bailiffs – Chamber of Court bailiffs of Luxembourg)
CdN	Chambre des Notaires (Self-regulatory body of notaries - Chamber of Notaries of Luxembourg)
CEIOPS	Committee of Insurance and Occupational Pensions Regulators
CFT	Countering the Financing of Terrorism
CI	Cabinet d'instruction près le tribunal d'arrondissement de Luxembourg et cabinet d'instruction près le tribunal d'arrondissement de Diekirch ensemble (or in English: Office of the examining magistrate of the Luxembourg District Court and Office of the examining magistrate of the Diekirch District Court together)
CNUE	Conseil des Notariats de l'Union européenne
CRF	Cellule de Renseignement Financier – Luxembourg's Financial Intelligence Unit
CRF magistrates	The magistrates heading the CRF
CRI	Commission Rogatoire Internationale - International letters rogatory
CRS	Common Reporting Standard
CSSF	Commission de Surveillance du Secteur Financier – Luxembourg's financial sector supervisor
Dealers in goods	Natural or legal persons trading in goods, only to the extent that the payments are made in cash in an amount of €10 000 or more whenever a transaction is executed in a single operation or in several operations which appear to be linked (2010 AML/CFT Law)
DNFPB	Designated Non-Financial Business or Profession
ECB	European Central Bank
EEA	European Economic Area
Egmont Group	Informal network of 151 FIUs for the stimulation of international co-operation
Egmont Group Charter	Egmont Group of Financial Intelligence Units Charter, as approved by the Egmont Group Heads of Financial Intelligence Units in July 2013
EMDDA	European Monitoring Centre for Drugs and Drug Addiction
EOI	Exchange of information
EU	European Union
Expert Comptable	Chartered Professional Accountants
FATF	Financial Action Task Force
FDI	Foreign Direct Investment
Freeport operators	Operators in a free zone authorized to carry out their activity pursuant to an authorization by the ADA within the Community control type 1 free zone located in the municipality of Niederanven Section B Senningen called Parishaff L-2315 Senningerberg (Hoehenhof)
FTE	Full-time equivalent
GDP	Gross Domestic Product
GDR	Grand-Ducal Regulation (règlement grand-ducal)
General State Prosecutor	Procureur Général d'Etat
Investigative Judge	Juge d'instruction
Investigative Office	Cabinet d'Instruction
IRE	Institute of statutory Auditeurs ("Institut des Réviseurs d'Entreprises", Self-regulatory body of statutory auditors and audit firms)
Judicial Police	Police Judicaire

JUR CC	CSSF AML/CFT-specialised legal department and AML/CFT central team (including coordination team)
LBR	Luxembourg Business Registers (or Registre de Commerce et des Sociétés)
MAEE	Ministère des Affaires étrangères et européennes (Ministry of Foreign and European Affairs)
Magistrats	Magistrates, i.e. according to Luxembourg law on judicial organization either Investigative Judges or Prosecutors
ML/TF	Money laundering and terrorist financing
MLA	Mutual Legal Assistance request (sometimes referred to as Legal Assistance Request (LAR) or Commission Rogatoire Internationale CRI)
MoF	Ministère des Finances (Ministry of Finance)
MoJ	Ministère de la Justice (Ministry of Justice)
MoS	Ministère d'État (Ministry of State)
Monitoring Committee	Comité de Suivi des Sanctions Financières Internationales (Monitoring Committee for International Financial Sanctions)
MoU	Memorandum of understanding
MVTS	Money and value transfer services (sometimes also referred to as Money service businesses, MBS)
New notice	New notice in case management system of the prosecution authorities (the JUCHA) based on intelligence received (e.g. from CRF or Police)
NGO	Non-governmental organisation, referring to ASBLs accredited by the MAEE as an NGO
NPC	National Prevention Committee (or Comité de prévention du blanchiment et du financement du terrorisme)
NPO	Non-profit organisation, referring to ASBLs
OAD	Ordre des Avocats de Diekirch (Self-regulatory body of lawyers of Diekirch)
OAL	Ordre des Avocats de Luxembourg (Self-regulatory body of lawyers of Luxembourg)
OEC	Ordre des Experts Comptables (Self-regulatory body of chartered professional accountant – Order of Chartered Professional Accountants)
OECD	Organization for Economic Cooperation and Development
OSI	On-site inspection department (CSSF)
PANC	Procédure administrative non contentieuse (Non-judicial administrative procedure)
Parquet d'arrondissement Diekirch or Luxembourg	State Prosecutors' Offices at the District level (Luxembourg and Diekirch)
PG	Parquet général du Grand-Duché de Luxembourg - General State Prosecutor's Office
Parquet Général Statistical Service	Statistical Service of prosecution authorities
PEP	Politically Exposed Person
Professionals	Professionals falling under the scope of the 2004 AML/CFT Law as defined in article 2 and subject to the professional obligations outlined under articles 3 to 8
Prosecution authorities	"Parquet d'arrondissement" or "Parquet général"
Prosecutor	Procureur
PSA	Insurance sector professionals
PFSs	Professionels du secteur financier – professionals as defined in the 1998 CSSF Law
RBA	Risk-Based Approach
RBAC	CSSF's Risk-Based Approach Committee
RBE	Register of Beneficial Owners (or Registre des bénéficiaires effectifs)
RCS	Registre des du Commerce et des Sociétés (now called Luxembourg Business Registers – LBR)

Réviseurs d'Entreprises, Réviseurs d'entreprises agréés, Cabinets de révision et cabinets de révision agréés	Statutory auditors, approved statutory auditors, audit firms and approved audit firms as defined in the 2016 Audit profession Law
SAR	Suspicious Activity Report
SARe	e-commerce related SAR
SICAR	Société d'investissement en capital à risque – Investment company in risk capital
SICAV	Société d'investissement à capital variable – Investment companies with variable capital
SME	Small and medium enterprises
SNRA	(EU's) Supra-national risk assessment
SPJ	Service de police judiciaire - Judicial Police Service
SRBs	Self-regulatory bodies
SRE	Service de Renseignement de l'Etat – Luxembourg State Intelligence Service
SSM	Single Supervisory Mechanism
State Prosecutor	Procureur d'Etat
STATEC	National Institute of Statistics and Economic Studies of the Grand-Duchy of Luxembourg
STR	Suspicious Transaction Report
STRe	e-commerce related STR
STRs	All types of reports, ie STR, SAR, STRe, SARe, TFTR, TFAR
Supervisory authorities	CSSF, CAA, AED, as defined in the 2004 AML/CFT Law, Art. 1 (16)
TCSP	Trust & Corporate Service Provider (or Prestataire de services aux trusts et aux sociétés)
TF	Terrorist financing
TFAR	Terrorist Financing Activity Report
TFTR	Terrorist Financing Transaction Report
UBO	Ultimate beneficial owner
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNSCR	United Nations Security Council Resolution
VAs	Virtual Assets
VASPs	Virtual Assets Service Providers
WGs	Working Groups