cssf

Commission de Surveillance
du Secteur Financier

Private Banking Sub-Sector Risk Assessment

2023 Update

CONTENTS

Foreword

Since the initial publication of the Private Banking Sub-Sector Risk Assessment in 2019, CSSF's and the private sector's understanding of money laundering and terrorist financing risks in private banking in Luxembourg has continuously improved.

This has been favoured by the public private partnership put in place with the Luxembourg Bankers' Association, private banks and the Luxembourg FIU, which has created a forum where money laundering, terrorism financing and proliferation financing risks are discussed to the mutual benefit of its members.

Luxembourg is one of the leading international financial centres in the world, a position to which private banking has significantly contributed over the years.

The growth of the financial sector overall, and private banking in particular, increases Luxembourg's exposure to the evolving threat of money laundering and terrorism financing. Whilst the financial services sector as a whole is exposed, private banking activities are particularly and specifically at risk when it comes to money laundering. This has been highlighted in all iterations of the National Risk Assessment since its first publication in 2018, confirming similar findings by the FATF or the most recent European Commission's Supra-National Risk Assessment, dated October 2022, and by supervisors in many other countries.

Luxembourg in general, CSSF in particular, but also private banks have committed significant resources to combatting the money laundering and terrorism financing risks. Over the years, Luxembourg's AML/CFT framework has been continuously strengthened, the country's understanding of its ML/TF risks has been deepened and refined and the effectiveness of mitigating and preventive measures considerably enhanced. These efforts were also recognised during the FATF's recent review of Luxembourg and the Mutual Evaluation Report published in September 2023.

The Private Banking Sub-Sector Risk Assessment and the work done by the Expert Working Group on Private Banking are cornerstones of Luxembourg's efforts to continuously maintain and improve its understanding of financial sector risks and are a key tool for all private banking stakeholders, to better understand the money laundering and also terrorism financing risks associated with private banking, and the measures necessary to combat them. I would like to express the CSSF's thanks to the members of the group for their contributions, and in particular the Luxembourg FIU for sharing its experience through a series of case studies which contribute to a better understanding of some of the threats described herein.

Supervised entities are expected to use this risk assessment to review and strengthen their understanding of ML/TF threats and vulnerabilities and further contribute towards the development of proportionate and effective controls.

While some potential areas for further improvement have been identified, the recent Mutual Evaluation Report shows that Luxembourg is on the right path and has made substantial progress during the past years. And with new risks emerging, there is no time for standing still. CSSF will continue its efforts to maintain and further enhance its AML/CFT supervision and expects the private banking sub-sector and all entities that are under its supervision to do the same, in order to minimise risk to themselves and the Luxembourg economy, preserve Luxembourg's reputation as an international financial centre and ensure a solid foundation for its continued development.

Claude Wampach

Director, CSSF

1. INTRODUCTION

The Financial Action Task Force (FATF) recurrently highlights private banking as a sector particularly exposed to money laundering (ML). This view is echoed in the European Commission's Supranational Risk Assessment (SNRA), by supervisors in many countries as well as Luxembourg's own National Risk Assessment (NRA).

In Luxembourg, private banking is an important part of the country's banking sector.[1] The sub-sector has been highlighted as having a "very high" inherent ML risk in the 2018 National Risk Assessment (NRA), and again in the updated NRA of 2020. Consequently, CSSF completed a first, dedicated Private Banking Sub-Sector Risk Assessment (PBSSRA) in December 2019, to identify more precisely which aspects of private banking activities are particularly exposed to money laundering/terrorism financing (ML/TF).

This risk assessment revisits, and updates where necessary, the conclusions of the 2019 assessment. CSSF Banking Supervision has led this assessment, in close cooperation with the Supervision of Investment Firms department, the Luxembourg FIU (CRF), the Luxembourg Bankers Association (ABBL) and the Expert Working Group (EWG) on ML/TF risks in private banking.

New additions to the PBSSRA include a revised section on TF risk. TF-linked threats in private banking have been reassessed in section 4.3 in light of the 2022 publications of the updated SNRA and Luxembourg's first Terrorism Financing Vertical Risk Assessment (TFVRA), in line with a recommendation by the FATF.

Furthermore, a new Chapter 7 has been inserted, to address emerging and increasing areas of ML/TF risk identified by CSSF, including a section focussing on financial sanctions. Further areas that were reviewed include outsourcing, new technologies and virtual assets. Section 7.5 draws attention to professional money launderers, who insert themselves in the money laundering process as an additional layer, thus rendering detection even more difficult.

Finally, Chapter 8 revisits and updates the recommendations for the private sector, based on conclusions from CSSF's supervision, and highlights some of CSSF's present and future initiatives.

1.1. International ML/TF context for private banking

Before considering the specifics of the private banking sub-sector in Luxembourg, it is useful to have a look at private banking internationally. FATF has identified several areas of ML risks in wealth management, including: "culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions [and] multiple jurisdictions".[2] FATF encourages private banks[3] to understand the different ML/TF risks associated with their clients and activities and take appropriate mitigating actions. FATF also states that "private banking accounts can be attractive to money launderers and particularly those wishing to launder the proceeds of corruption because of the high net worth of the customer, the offshore nature of many of the facilities offered, and the type of products and services available. These services are likely to attract money launderers who look for adequate ventures to move large sums of money without attracting notice."[4]

The 2022 SNRA highlights i.a. that "Given the combination of sophisticated financial products and services, and a wealthy customer base, which sometimes includes politically

[1] Luxembourg National Risk Assessment, 2020
[2] FATF, *Guidance for a Risk-Based Approach: the Banking Sector*, 2014
[3] "Private bank(s)" as used in this document refers to banks offering significant private banking services.
[4] FATF, *Specific Risk Factors in Laundering the Proceeds of Corruption*, June 2012

exposed persons (PEPs), the sector can be abused also for tax evasion, especially in cases where assets of the beneficial owners are hidden behind complex ownership structures and direct private banking customers are the associates or family members of the actual beneficial owners". The SNRA rates the ML threat related to private banking as "significant/very significant", an increase as compared to the 2017 SNRA referenced by the 2019 PBSSRA and a continuation of its assessment of 2019.[5]

A number of national supervisors have highlighted in the past the high inherent ML/TF risks in private banking, and the European Banking Authority (EBA) dedicated guideline 12 of its ML/TF Risk Factor Guidelines[6] entirely to the identification and prevention of wealth management/private banking related ML/TF risks.

1.2. Luxembourg ML/TF context for private banking

1.2.1. Luxembourg's National Risk Assessment

In December 2018, Luxembourg published its first NRA, which was updated in 2020. The purpose of the NRA is to identify, understand and assess the ML/TF risks to which the country is exposed, and inform, direct and support the national AML/CFT strategy.

Table 1: National exposure to ML/TF threats map from NRA[7]

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
Terrorism and terrorist financing	Medium	Medium	Medium

[5] European Commission, *Commission staff working document accompanying the REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, 2022

[6] EBA, *Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The ML/TF Risk Factors Guidelines"),* EBA/GL/2021/02 consolidated version, 2023

[7] Subsequently to the NRA's threat assessment, the Law of 20 July 2022, modifying the Law of 9 December 2020 on international financial sanctions regimes (Financial Sanctions Law), introduced in article 506-1 of the Luxembourg Criminal Code a new predicate offence relating to breaches of financial sanctions.

The NRA identifies predicate offences (threats) that are particularly relevant in Luxembourg. Starting from FATF's designated categories and using a weighted average of external and domestic exposure, the 2020 NRA concludes that fraud and forgery, tax crimes, and corruption and bribery are "very high" threats in Luxembourg, driven predominantly by the country's international nature and cross-border exposure. In contrast, and with the exception of fraud and forgery, the threat of ML from domestic crimes is much lower, due to Luxembourg's overall lower low crime rate and limited presence of organised crime.

The NRA also identifies and scores the inherent risk (i.e. risk before the application of mitigating factors) of the banking sector as inherently "high", and the private banking sub-sector as "very high" risk.

Table 2: Overview of Luxembourg's NRA – risks in the banking sector[8]

Sector		Inherent risk	Sub-sectors	
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

Following the publication of the updated NRA and the publication of Luxembourg's TFVRA in 2022, and considering its own experience accumulated since 2019, CSSF is now reviewing its sub-sector risk assessment of private banking. Sub-sector risk assessments bridge the gap between risk assessments at sector level (covered by the NRA) and entity level (covered by CSSF's supervision).

1.2.2. Private banking supervision in Luxembourg

CSSF is in charge of supervising the financial sector in Luxembourg and enforcing compliance with professional obligations related to AML/CFT by professionals. Within CSSF, Banking Supervision performs market entry controls and exercises ongoing AML/CFT and prudential supervision of all banks in Luxembourg.[9]

CSSF applies a risk-based approach to AML/CFT supervision, in line with FATF guidelines and recommendations. This involves identifying, assessing and understanding ML/TF risks faced by the banking sector, its specific products and services and the clients and jurisdictions it serves as well as taking AML/CFT measures commensurate to those risks.[10] CSSF regularly communicates to the private sector on AML/CFT obligations and ML/TF risks through regulations, circulars, bilateral communication, participation to industry events such as conferences, interaction with representative industry bodies and public-private partnerships (PPP).

ABBL has established in 2007 a dedicated private banking cluster to support the needs and development of players within the private banking sector in Luxembourg, via training, opinion building, working groups, position papers and other tools. In 2019 CSSF and ABBL established a joint Expert Working Group for AML/CFT in Private Banking (EWG PB), as a PPP.[11] This working group was joined in January 2020 by the Luxembourg FIU. The EWG meets on a regular basis to discuss AML/CFT topics and strengthen the framework to combat ML and TF in banks offering private banking services.

[8] Note, the NRA ranks risks on a five-point scale (Very High, High, Medium, Low, Very Low) – this risk assessment uses a four-point scale (High, Medium-High, Medium-Low, Low).
[9] Since November 2014, the licensing (including licence withdrawal and approval of qualifying holdings) of all new banks within the Eurozone is under the ultimate authority of the European Central Bank (ECB).
[10] FATF, *Guidance for a Risk-Based Approach: the Banking Sector*, 2014
[11] AML/CFT: The ABBL, the CRF and the CSSF sign a public-private partnership

1.2.3. Entities providing related services in Luxembourg

Whilst this document focuses primarily on private banks, some of the services described herein are also provided by other actors and in particular investment firms.[12] Since March 2023, representatives from the investment firms sector have also joined the EWG PB.

[12] Professionals of the Financial Sector that provide investment services or perform investment activities according to art. 24-1 to 24-9 of the Law of 5 April 1993 (LFS).

2. STAKEHOLDERS, METHODOLOGY AND DATA

This section describes the stakeholders involved in the risk assessment and the methodology and data used.

2.1. Stakeholders in this assessment

This document was written by CSSF's **AML/CFT Banking Supervision** in close collaboration with other departments and internal experts as well as after consultation of the EWG PB, which brings together representatives from private banks, investment firms[13], ABBL, the CRF and CSSF.

2.2. Methodology of the assessment

The assessment identifies relevant ML/TF threats and potential areas of vulnerability to evaluate risk and assesses residual risk following the mitigating measures put in place by both CSSF and the private sector. The methodology is closely aligned to that used in Luxembourg's NRA. The methodology is also aligned to the revised Guidelines on Risk-Based Supervision[14] and Guidelines on ML/TF Risk Factors[15], to FATF Guidance and to peer practices.

General approach[16]

In its guidance for national money laundering and terrorist financing risk assessments, the FATF has defined **risk** as a function of three factors: **threat**, **vulnerability** and **consequence**.

Inherent risk – Threat assessment

The FATF defines a **threat** as "a person or group of people, an object or activity with the potential to cause harm. 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" (predicate offences).

The objective of this threat assessment is to understand the environment in which predicate offences are committed, to identify their nature, and to assess the exposure of private banking to them.

This document examines the most relevant ML threats for private banking, building on the conclusions of the NRA.[17]

Note: TF specific threats are presented separately in section 4.3. In line with the SNRA and the NRA, as well as the TFVRA dated May 2022, this assessment highlights the overall low prevalence of TF via private banking and provides reasons behind this observation.

[13] Investment firms participate in the EWG PB since March 2023.
[14] EBA, *The Risk-Based Supervision Guidelines,* EBA/GL/2021/16, 2021
[15] EBA, *The ML/TF Risk Factors Guidelines*, EBA/GL/2021/02 consolidated version, 2023
[16] This section contains extracts and abbreviated quotes from the FATF's Guidance for national money laundering and terrorist financing risk assessments.
[17] NRA, 2020

Inherent risk – vulnerability assessment

According to the FATF, **vulnerability** refers to "those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities as distinct from threats means focussing on, for example, weaknesses in AML/CFT systems or controls or certain features of a country, sector, product or service that make them attractive for ML or TF purposes".

Vulnerabilities determine thus the relative attractiveness of a sector or sub-sector for ML/TF purposes. Vulnerability arises from activities which are particularly exposed to abuse or misuse for ML/TF purposes. Vulnerability in private banking is driven by multiple factors, including the international nature of the sector and its clients, the volume of cross-border flows and their size, the intervention of intermediaries, its structure, products and services offered, or the involvement of external advisors.

Consequence refers to the impact or harm that ML or TF may cause on financial systems and institutions, as well as the economy and society more generally. Consequences include financial losses and fines suffered by an institution, public shaming, loss of confidence and trust in the institution or the sub-sector or sector as a whole, up to economic, political, societal, durable reputational damages at country level and beyond.

The main objective of this assessment is to determine the level of ML/TF risk posed by different private banking activities.

Mitigating factors and residual risk assessment

Mitigating factors are all the elements in place that contribute to combating ML/TF. This includes both private sector controls (e.g. internal control frameworks and systems) as well as public measures (e.g. legal, judicial, supervisory and institutional frameworks) in place to reduce and prevent ML/TF risks.

Mitigating measures cover the full lifecycle of supervision: understanding of ML/TF risks, market entry (including licensing, qualifying holding procedures, registration and fitness and propriety checks), rules setting and oversight, assessment of compliance with rules and enforcement.

Residual risk is the risk of ML/TF occurring after considering mitigating factors in place. The level of residual risk of the sub-sector is determined by reducing the level of inherent risk by an amount commensurate with the strength of mitigating factors. Note, if residual risk and inherent risk scores are the same, this does not mean that there are no mitigating measures in place (only that the mitigating measures do not reduce inherent risk substantially).

2.3. Data and limitations

This assessment uses both quantitative and qualitative data from a variety of relevant sources. These include international sources (e.g. international organisations, foreign competent authorities, industry bodies, academia), data published by the ABBL's private banking cluster, data from other domestic competent authorities (e.g. CRF), CSSF internal data collected as part of supervisory measures, information exchanged with the EWG PB as well as other information provided by the private sector (e.g. via surveys, interviews or workshops). Where information was missing or incomplete, the assessed level of risk has been increased, in line with a conservative approach recommended by FATF.

3. LUXEMBOURG PRIVATE BANKING ECOSYSTEM

Luxembourg's private banking sub-sector is quite fragmented, with the largest ten private banks holding a market share of close to 70%, and many smaller institutions.[18] Some offer exclusively private banking services, others have more of a mixed business model, offering other services alongside private banking. Most private banks in Luxembourg are foreign-owned and operate in Luxembourg as part of European and international groups.[19]

Since 2015, the number of private banks has been decreasing by 25%, reflecting a growing sector consolidation and the pressure especially on smaller banks from increasing costs and a highly competitive environment. Nevertheless, private banking remains an important component of Luxembourg's banking sector.[20]

Taxonomy

This assessment has split the different actors of the private banking ecosystem into five categories:

Table 3: Actor taxonomy for the purpose of this private banking sub-sector risk assessment

Actor category	Description of actor's role
Private banks	Private banks are banks that provide personal banking services and tailor-made products to their clients. Private banks typically provide two main categories of activities: asset management (i.e. custody of financial assets and investment services) and ancillary services (i.e. current account banking, credit solutions, wealth structuring and insurance solutions).
Investment firms	Investment firms are a category of professionals of the financial sector defined in Articles 24-1 to 24-9 of the LFS. Investment firms can be authorised to provide different services, including portfolio management, investment advisory and some ancillary services, comparable to private banks.
Clients	Clients include both direct clients (i.e. account-holders) and ultimate beneficiaries. They show different characteristics based on the value of their assets under management, the geographic origin of their assets, and their legal structure. Ultimate beneficiaries are natural persons who are the ultimate source of funds or who ultimately own the assets and benefit from private banking activities.

[18] ABBL data, 2023
[19] CSSF internal data, 31 December 2023
[20] KPMG-ABBL, *Clarity on performance of Luxembourg private banks,* 2022-2023

Intermediaries	Intermediaries facilitate interactions between private banks/investment firms and clients and often maintain a regular relationship with the private bank/investment firm or the client. For example, the actors in this category could be: Power of Attorney (POA) holders carrying out instructions on behalf of the client, such as signing documents; business introducers helping banks grow their client base; or third party managers managing the client's assets.
External service providers	External service providers are specialists that support clients and/or private banks/investment firms with specialised services provided at specific occasions. For example, they can provide financial or legal expertise, trust or company services or assist private banks/investment firms with specific aspects of client due diligence.

3.1. Private banks

Private banks provide diverse, personalised wealth management services. For the purpose of this assessment, these activities have been split into two core categories of asset management services and four categories of ancillary services.[21]

Table 4: Activity taxonomy for private banking banks

Categories	Taxonomy elements	Description
Asset management	**Custody of financial assets**	Booking and safekeeping of financial assets along with all related back-office services, such as for instance transaction execution (e.g. brokerage services) and settlement, dividend and interest collection and distribution, corporate action processing or tax reporting.
	Investment services	Optimising clients' financial investments according to agreed objectives. There are two main kinds of investment services provided in Luxembourg: discretionary asset management services and investment advisory.[22,23,24]
Ancillary services	**Current account banking**	Providing services meant to satisfy clients' day-to-day banking needs, such as current accounts, payment

[21] This is an illustrative categorisation defined for the purpose of this risk assessment.
[22] Discretionary asset management services are investment services and products provided by a private bank while following the risk tolerance and the financial requirements agreed in advance with the client. The private bank manages investments on behalf of the client, who typically cannot ask for specific investment decisions (e.g. buying stocks from a specific company).
[23] Investment advisory refers to the provision of advice on investments related to the client's portfolio (e.g. monitoring of markets, private equity, debt products).
[24] Note, in recent years, some banks have added robo-advisors to their service offer. A robo-advisor is a digital tool that provides automated financial planning and investment services with little to no human supervision.

	services, credit cards or electronic banking
Credit solutions	Credit solutions typically include the provision of credit lines to improve portfolio returns as well as loans and mortgages unrelated to portfolio investments.
Wealth structuring	Advising in particular High Net Worth (HNW) and Ultra-High Net Worth (UHNW) clients on their investment strategy and on the most appropriate legal or fiscal structure to fit the client's needs for asset protection, succession planning or tax planning. It also includes creating bespoken personalised investment schemes. Wealth structuring is often offered by external advisors.
Insurance solutions	Distributing life and non-life insurance solutions to clients structured by licensed insurance professionals. In Luxembourg, insurance professionals are supervised by the Commissariat Aux Assurances (CAA).

3.2. Investment firms

Investment firms are supervised by the Supervision of Investment Firms department within CSSF.

Investment firms comprise different types of professionals and can provide a range of services comparable to private banks, including portfolio management, investment advisory services and some ancillary services.[25]

Wherever investment firms carry out private banking activities as described in this risk assessment, they are exposed to the same threats and present the same vulnerabilities as private banks.[26]

Accordingly, those relevant sections of this private banking assessment are, mutatis mutandis, applicable to investment firms as well.

3.3. Clients

Private banking clients can be natural persons, legal entities or legal arrangements.[27]

Private banking clients may also be categorised according to multiple additional criteria to understand and evaluate the level of ML/TF risk. For example, they can be analysed

[25] Due to the nature of the license held by investment firms, they cannot provide current account banking services, credit solutions, or insurance solutions.
[26] Refer to Annex B for further information regarding investment firms.
[27] Refer to the section on taxonomy at the beginning of Chapter 3.

according to their fiscal residency, nationality, source of wealth (e.g. wealth derived from inheritance or a family business), geographical spread of business operations, investment behaviour, etc.[28]

The industry is specialised in cross-border services, with some 80% of private banking clients having their fiscal residence outside Luxembourg. The client base remains nevertheless largely European.

According to the ABBL, the number of private banking accounts in Luxembourg has decreased from some 255,000 in 2012 to about 152,000 at the end of 2021[29]. However, while the share of affluent clients has continuously decreased, at the same time, the importance of HNW/UHNW clients has increased.[30]

As a result, despite an apparent loss of clients, the total value of assets under management (AuM) by private banks in Luxembourg has steadily grown since the 2008 financial crisis, from EUR 225 billion in 2008 to EUR 585 billion at the end of 2022. The 2022 figure represents an increase of 61% over the data used in the 2019 PBSSRA, and of 160% since 2008.[31,32]

The **geographic origin** of private banking clients in Luxembourg is diverse. Approximately 20% of private banking clients come from Luxembourg, while the remainder come from abroad. Of the latter, approximately 20% originate from Luxembourg's direct neighbouring countries, while over 40% are from other European countries.[33] The remaining share is very international, with a notable presence of clients from Latin America and the Middle East. Typical motivations for foreign investors to hold their assets in Luxembourg are the stable political, economic and juridical environment, the strong property protection, the well-regulated and stable financial sector providing numerous investment opportunities, the central European location including membership of the Eurozone, the diverse and high-quality services, the concentration of experts and the international, multi-lingual workforce.

[28] Many other categorisations can exist and their appropriateness may depend on banks' specific business models.
[29] ABBL data
[30] Refer to *Figure 3: Evolution of the distribution of client wealth bands.*
[31] KPMG-ABBL, *Clarity on performance of Luxembourg private banks,* 2023
[32] According to ABBL, the total private banking AuM dropped slightly in 2022 as compared to 2021, due to geopolitical turbulence, supply chain constraints, fears of recession and tightening of monetary policy.
[33] Based on: KPMG-ABBL, *Clarity on performance of Luxembourg private banks,* 2023

Figure 1: Geographical origin of PB clients [34]

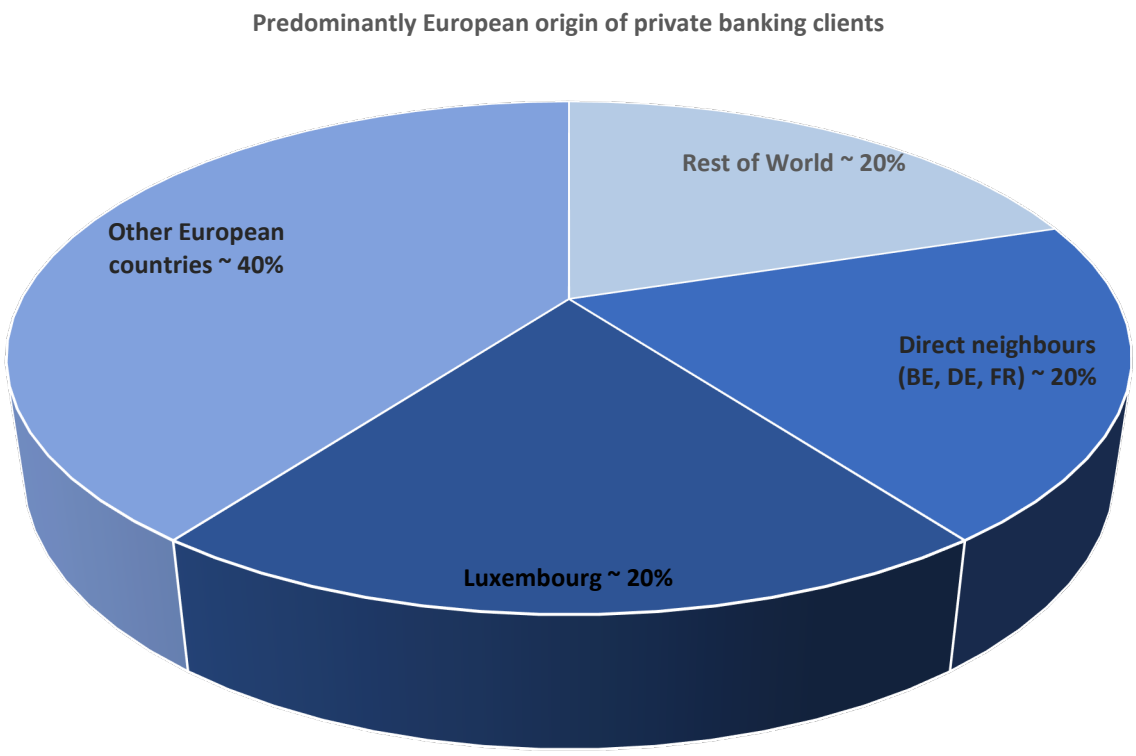
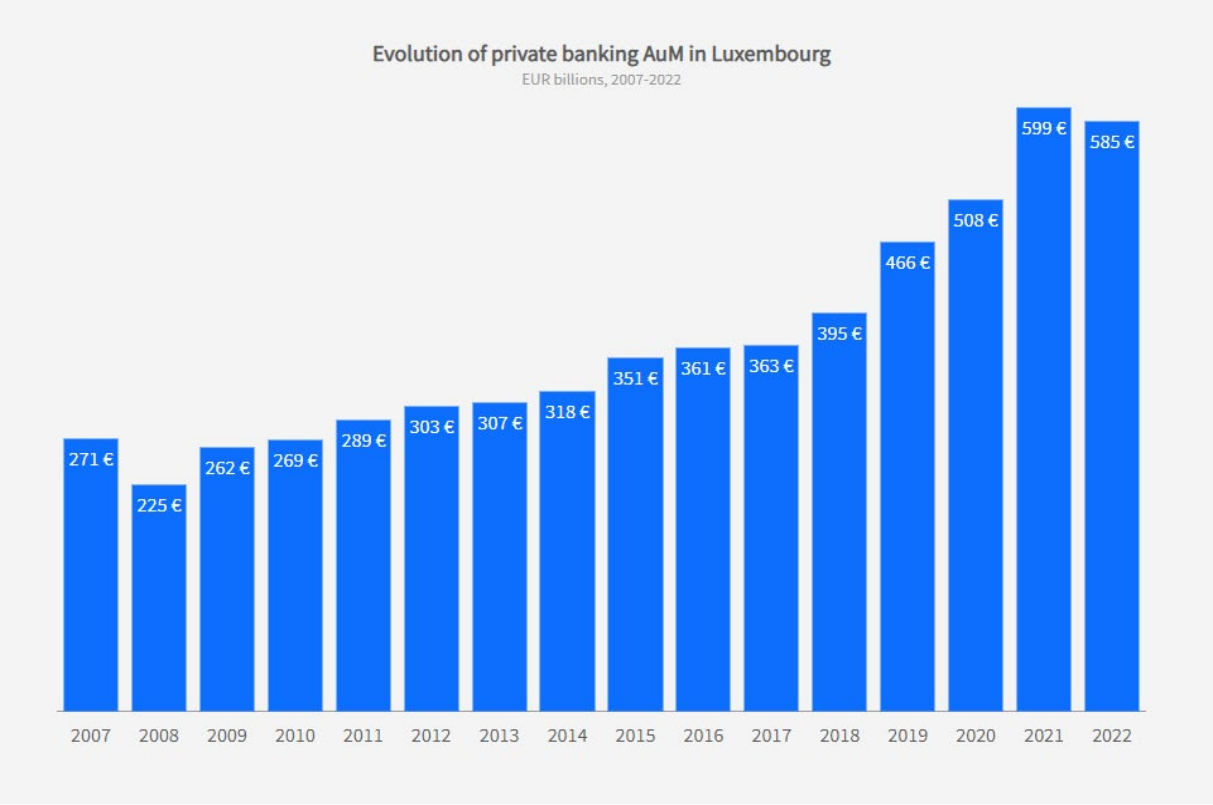


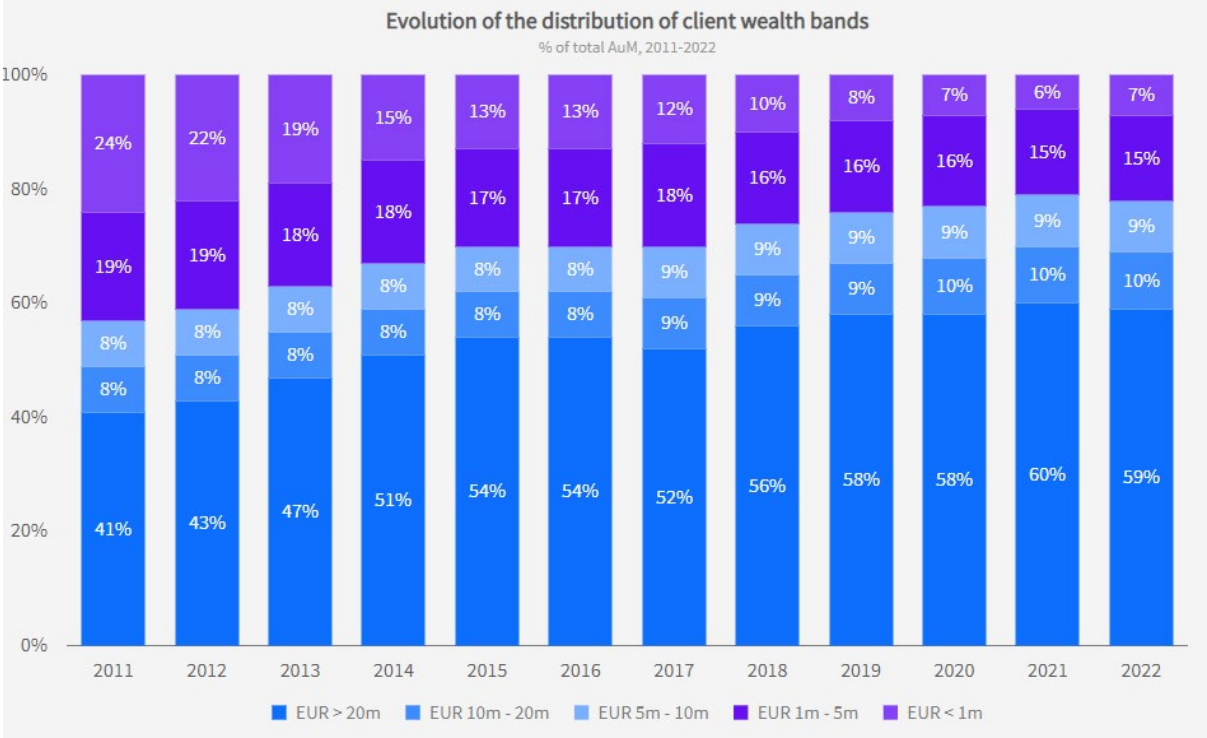
Figure 2: Evolution of private banking AuM in Luxembourg [35]



[34] Based on: KPMG-ABBL, *Clarity on performance of Luxembourg private banks,* 2023

The 2023 KPMG-ABBL Private Banking Report categorised private banking clients into 5 wealth bands, ranging from below EUR 1 million AuM to above EUR 20 million AuM. The survey showed that, whereas the share of the middle wealth bands (EUR 5 – 20 million) in the sub-sector's total AuM has remained relatively stable over the years, the importance of the two lower wealth bands has been steadily and considerably declining whereas the top wealth band (> EUR 20 MM) makes up for 59% of the sub-sector's AuM and drives the sector's growth[35].

Figure 3: Evolution of the distribution of client wealth bands, % of total AuM (2011-2022)[36]



3.4. Intermediaries

Intermediaries interact between clients and private banks at different stages of the private banking value chain. Intermediaries active in Luxembourg's private banking sub-sector include business introducers, POA-holders, and third-party managers.[37]

Business introducers are natural persons or legal entities increasing private banks' reach, helping them to grow their client base.[38] They may be lawyers, financial advisors, accountants, asset managers or other financial institutions. They typically have a professional relationship with the bank that is subject to an agreement setting out the responsibilities of the bank and the introducing intermediary. To some extent, private banks may also rely on intermediaries to provide inputs to conduct client due diligence (CDD), e.g. when collecting client documentation. Private banks that are subsidiaries or branches of foreign-owned banks may benefit from their parent or other group companies to grow their client base through referrals of clients. While these group companies may

[35] KPMG-ABBL, *Clarity on performance of Luxembourg private banks*, 2023
[36] KPMG-ABBL, *Clarity on performance of Luxembourg private banks*, 2023
[37] Please note that this is an illustrative categorisation defined for the purpose of this risk assessment. Additional intermediaries may exist, and some of these activities may be performed by the same intermediary.
[38] Also referred as "business finders" or third-party introducers, as defined in The Wolfsberg Group's *The Wolfsberg AML Principles Frequently Asked Questions with Regard to Intermediaries,* 2012.

also provide inputs for CDD on those clients, the private bank in Luxembourg remains ultimately responsible for the due diligence.

POA-holders can be individuals or legal entities with, for example, signatory authority over an account or on behalf of a beneficial owner but that do not act on a professional basis as an asset manager. For example, they may be lawyers or accountants, but also family members or trusted individuals representing the account holder or the ultimate beneficiary of the account. When the account holder is not a natural person, the ultimate beneficiary could also act as a POA-holder.

Third-party managers are professional asset managers, typically investment firms providing discretionary management or advisory services to clients. They may be located in Luxembourg or abroad. In most countries, including Luxembourg, asset management services can only be provided by licensed professionals.

3.5. External service providers

For the purpose of this assessment, external advisors are third-party specialist service providers that support clients and/or private banks with specific, highly specialised services.[39] For example, these can include legal, financial, tax, TCSP or due diligence-related services.[40]

Financial advisory services: External professionals with specialist financial expertise may provide specific or tailored services to private banks and/or clients. Such financial experts can include external asset managers (e.g. private equity funds), economic advisors (e.g. merger and acquisitions advisors and corporate finance advisors), accountants, auditors, insurers and real estate agents.

Tax advisory services: Specialised tax advisors often advise private banking clients, especially in the higher wealth bands, on tax efficient investment, wealth or estate planning strategies. Tax advisors may also be authorised to provide other services, or work closely together with other professionals, such as lawyers.

TCSP services: Clients or private banks themselves may also request support from trust and company service providers to optimise relevant investments or wealth structuring strategies. According to the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended (AML/CFT Law) and in line with FATF's definition, there are five types of trust and company services:[41,42]

- Incorporation services consist of forming companies or other legal persons.
- Representation services include 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.[43]
- Domiciliation services include 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.

[39] There are other service providers that also support private banks but are less specific to private banking activities (e.g. Information Technology vendors, Human Resources providers). Such providers are out of the scope of this report.
[40] Please note that this is an illustrative categorisation defined for the purpose of this risk assessment. Additional specialist services may exist, and some of these may be performed by the same professional.
[41] Luxembourg, *AML/CFT Law Chapter 1, Article 1, Paragraph 8(a) to 8(e)*
[42] FATF, *Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems*, 2021
[43] Note that true "nominee directors" do not exist under Luxembourg company law. All appointed directors share the same obligations and responsibilities.

- Fiduciary/trustee services correspond to companies 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, and
- Shareholder proxy services consist in acting as, or arranging for another person to act as, a shareholder representative or proxy.[44]

Several types of professionals can perform trust or company services. A number of these are supervised by CSSF, such as banks, investment firms, management companies or specialised professionals of the financial sector (among which family offices).

Legal advisory services: Lawyers provide legal advice and set up contracts and agreements, and notaries create the investment vehicles or other corporate or legal structures to implement the client's tax, estate planning or investment strategies.[45]

Client due diligence services: Private banks may leverage third parties to get assistance when performing specific due diligence requirements or screening prospects and existing customers, such as HNW/UHNW customers. Private banks may request external expertise or group capabilities on specific CDD inputs (e.g. due diligence reports, access to specialised due diligence database, information on source of wealth) or may leverage clients' documentation in possession of intra-group competence centres to fulfil due diligence requirements. Nevertheless, private banks remain ultimately responsible for the due diligence. As discussed above, introducing intermediaries may also conduct part of the CDD.

[44] Note that true "nominee shareholders" do not exist under Luxembourg law; while shareholder proxies or representatives may be appointed in certain circumstances, the identity of the true shareholder must be disclosed.

[45] FATF defines legal professionals as "Lawyers, notaries and other independent legal professionals – this refers to sole practitioners, partners, or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures", FATF, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, 2013.

4. INHERENT RISK – THREAT ASSESSMENT

The purpose of this section is to understand and to review the exposure of private banking activities to ML/TF threats[46] in general, and to determine and assess those ML/TF threats that are most relevant for private banking in Luxembourg.

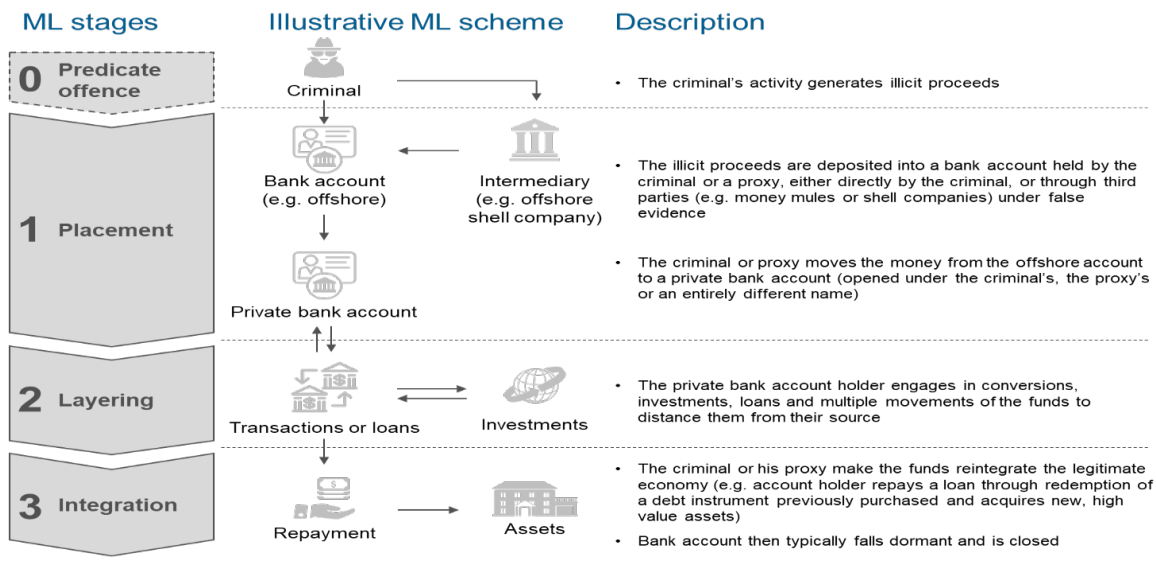
4.1. Private banking's exposure to money laundering globally

Private banks are exposed to ML during all stages: placement, layering and integration.[47] Placement is the initial entry of illicit proceeds into the financial system. Layering involves using complex movement of funds to distance the illicit money from the source. Integration involves returning money to the criminal from what seem to be legitimate sources.

At the **placement stage**, private banks are exposed to multiple ways in which illicit proceeds can be placed in the financial system, for example, cash deposits, cheques, or money orders. Historically, cash was more commonly used by criminals because it is difficult to ascertain the source of funds and can be impossible to know the intended beneficiary. Private banks can be abused or misused as the point of entrance of their clients' illicit cash to the financial market.

However, private banks' primary exposure is during the **layering** and **integration** stages. Criminals may abuse or misuse sophisticated investment services to obscure the audit trail and sever the link with the original crime. During these stages, funds are typically transferred electronically from one investment or account to another and potentially across several geographies. Eventually, funds are returned in one form or other to the criminal, from what seem to be legitimate sources.

Figure 4: Illustration of ML scheme through private banking



The exposure of private banks to layering and integration is due to multiple factors, among which the following are considered particularly relevant:

- **Objectives of the business:** Wealth preservation is a goal shared by the criminal as well as the portfolio manager to whom the funds are entrusted, which makes the

[46] "Risk can be seen as a function of three factors: threat, vulnerability and consequence", FATF, *National Money Laundering and Terrorist Financing Risk Assessment,* 2013.
[47] FATF, *FAQ:* How is money laundered ?

simulation of legitimate investor behaviour easier and facilitates the establishment of a relationship.

- **High value of investments and transactions:** Private banking clients are by nature wealthy and invest larger amounts of funds. Large value transactions are likely to occur more frequently in private banking than in other banking sectors, making an unusual and illicit nature of large transfers more difficult to detect and facilitating the introduction of large sums into the financial system.
- **International nature of the business:** The international nature of private banking increases the likelihood of dealing with illicit proceeds from predicate offences committed in foreign jurisdictions, in particular when in contact with high-risk jurisdictions. This can be exacerbated by the use of (foreign) intermediaries that create distance between the client and the private bank.
- **Complexity of some products and schemes used in private banking and wealth management:** The inherent complexity of some products and schemes used to serve clients' needs (e.g. for wealth preservation or tax planning by HNW/UHNW clients), can increase the opaqueness of client relationships and increase the difficulty in detecting ML.
- **Difficulty in identifying beneficial owners:** The use of legal entities or legal arrangements can increase the difficulty of identifying beneficial owners.[48] Complex legal structures might be used by criminals to hide their identity or the role of beneficial owners.

4.2. ML threats most relevant for private banking in Luxembourg

When considering the 2018 and 2020 NRAs' conclusions, discussions held during working groups, Suspicious Transaction / Suspicious Activity reporting data and CSSF's off- and onsite supervisory experience, the following three predicate offences appear as particularly relevant threats for the private banking sub-sector in Luxembourg: (1) tax crimes; (2) fraud; and (3) corruption and bribery. Luxembourg is typically not the country of origin of tax crimes or corruption offences, although the country is exposed to some level of domestic fraud. Also, typically, private banks in Luxembourg are at risk of ML especially at the layering and integration stages.[49]

The following sub-sections focus on these three threats and assess the specific exposure of the private banking sub-sector in Luxembourg. Occasionally, taking into account that predicate offences are committed more often abroad, information from global sources may be used to complement more limited, Luxembourg-specific data.

[48] A register of beneficial owners was set up by the law dated 13 January 2019 with effect from 1 March 2019 implementing provisions of the fourth Anti-Money Laundering Directive into Luxembourg law (*Loi instituant un Registre des bénéficiaires effectifs*). In order to protect legitimate privacy concerns, the Court of Justice of the European Union (CJEU) subsequently limited access to such registers on a legitimate need-to-know basis.
[49] NRA, 2020. Note, it is at these two stages that the CRF most commonly receives STRs or other information from Luxembourg-based institutions.

4.2.1. Tax crimes

Tax crimes involve the intentional breach of law to evade tax. Across the world, these crimes are one of the main sources of criminal proceeds and have been highlighted in the SNRA as particularly relevant for private banking.[50] Tax evasion (*escroquerie fiscale*) and aggravated tax fraud (*fraude fiscale aggravée*) are predicate offences in Luxembourg.[51,52]

The international nature of Luxembourg private banks' operations is one of the primary drivers of the sub-sector's exposure to misuse/abuse related to tax crimes.[53] In particular, the diverse geographic origin of private banking assets and clients exposes Luxembourg to the risk that *foreign* individuals may misuse/abuse private banks for tax evasion/fraud.[54] In contrast, misuse/abuse related to *domestic* tax evasion/fraud is assessed to be much lower. This is due to Luxembourg's tax system and small shadow economy (domestic tax evasion is estimated to be lower in Luxembourg than most other OECD countries, ~0.9% of GDP vs. 1-1.1% in Germany, France and Belgium).[55] The relative exposure to tax crimes from foreign and domestic individuals is also reflected in the nature of cases investigated by the CRF, as shown in the case study below.

Figure 5: Case study of suspicious activity in banking related to possible tax crimes[56]

The present case study is based on suspicious transactions (ST) involving Luxembourg based companies (LuxCos) and an unregulated Luxembourg securitisation vehicle presenting the following suspicious activities: (i) numerous cash withdrawals of low amounts generally not exceeding the EUR 10,000 threshold, (ii) transfers of part of the LuxCos' securities portfolios to an external asset manager's omnibus account in Luxembourg, or (iii) purchase of gold bars and their physical delivery.

Initial findings:

i. The securitisation vehicle had been set up in December 2016 by a TCSP.

ii. The two directors, shareholders and UBOs of the TCSP, both Luxembourg residents, had subscribed the securitisation vehicle's shares, acted as its directors and then later also registered as its ultimate beneficial owners (UBOs).

iii. The securities portfolios held by the LuxCos were initially held directly by a number of unrelated foreign natural and legal persons (Persons) and these securities portfolios had not been declared to the relevant foreign tax authorities. In December 2014, the aforementioned TCSP had set up the LuxCos to hold the securities portfolios in consideration for shares issued to the relevant Persons. In December 2016, the Persons transferred their

[50] European Commission, *Commission staff working document accompanying the REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities,* 2022

[51] Law of 23 December 2016 and Circular CSSF 17/650, 2017

[52] Aggravated tax fraud is defined according to the tax thresholds evaded or the level of reimbursement obtained. For tax evasion, increased gravity is related both to the amounts involved and the fact that means have been employed with a view to deceiving the tax authorities. Both offences related both to direct taxes (e.g. income and inheritance tax) and indirect taxes (VAT).

[53] This includes both the laundering of the proceeds of tax crimes, and the use of private banks' products and services to facilitate the tax crime itself.

[54] See Section 5.1.1 for further details on inherent risk related to 'Clients and Geographies'.

[55] CESifo Group, *Size and Development of Tax Evasion in 38 OECD Countries,* 2012. The shadow economy includes "all market-based legal productions of goods and services that are deliberately concealed from public authorities for the following reasons: avoid payment of taxes, avoid payment of social security contributions, avoid certain legal labour market standards and avoid complying with certain administrative procedures" (CESifo, F. Schneider, *Estimating the size of the shadow economies*, December 2016)

[56] Case study provided by the CRF

shares in the LuxCos via separate purchase agreements to the securitisation vehicle.

iv. Numerous partial redemptions of the securitisation vehicle's notes by various Persons thus indicating that the Persons, being the former beneficial owners of the securities portfolios, still had control over them. The red flags outlined in (i) to (iii) above are an additional indicator that the securitised LuxCos' shares were still under the control of the Persons who appeared to repatriate their undeclared funds after having channelled them through a corporate structure in Luxembourg.

Outcome:

The apparent lack of an economic rationale for setting up the LuxCos and later on selling their shares in the LuxCos to the securitisation vehicle in exchange for notes is in itself not illegal. But put in the context of the amendments to Luxembourg's legal framework on the common reporting standards for the automatic exchange of tax information on a European level, this increased layering of corporate structures over time between the Persons and their securities portfolios, from being held directly or through offshore structures in private banks to becoming noteholders in a securitisation vehicle, is a serious indicator of tax fraud given that as a result of these changes the foreign UBOs had effectively been removed from the OECD's Common Reporting Standard (CRS) scope.

Indeed:

In January 2015, Luxembourg started to exchange bank account data (on financial revenues) of non-resident natural persons with other EU countries, but corporate accounts remained out-of-scope. As a result, by transferring their securities portfolios from a private account (resp. offshore company account) to a corporate account in late 2014, the Persons could avoid the reporting of the securities portfolios to their competent tax authorities.

In January 2017, passive Non-Financial Foreign Entities (NFFEs) also fell within the scope of the CRS. The more comprehensive automatic exchange of information in tax matters includes, among other things, the exchange of information relating to financial accounts held in Luxembourg by (i) individuals resident abroad and (ii) certain legal entities with economic beneficiaries resident abroad. The first exchanges took place in 2017. The LuxCos were so-called passive companies (of the SOPARFI type) and had foreign residents as beneficial owners, therefore information relating to the bank accounts of the LuxCos and their beneficial owners should have fallen within the scope of this new law.

However, in December 2016, just before the more extensive automatic exchange of information came into force, the Luxembourg securitisation vehicle was set up. As previously mentioned, the 2 UBOs of the TCSP, both Luxembourg residents, had registered as beneficial owners of the securitisation vehicle and the LuxCos. As a result, the structure and its true beneficial owners (i.e. the Persons) no longer fell within the scope of the new law on the more comprehensive automatic exchange of information.

Red flags:

- Complex ownership structure
- Frequent changes in the ownership structure including beneficial ownership shift to out-of-scope individuals
- Corporate structure changes shortly prior to legislative changes on the common reporting standards

- Unknown/ poorly documented origin of funds
- Cash withdrawals of low amounts generally not exceeding EUR 10,000 threshold

Since 2017, annual statistics show that more than 40% of traditional banks'[57] Suspicious Transaction and Suspicious Activity Reports (STR/SAR) pertaining to fiscal offences are consistently filed by private banks each year, although the number of accounts and transactions of the sub-sector is much lower than that of other sub-sectors, such as retail for instance.

The data also shows that fiscal offences remain the predicate offence with the highest exposure level for private banks in Luxembourg.

Nevertheless, this high number of STR/SAR related to tax offences also illustrates the positive impact of adding tax evasion *(escroquerie fiscale)* and aggravated tax fraud (*fraude fiscale aggravée)* to the list of predicate offences for ML. Private banks in particular are today very much aware of this risk and have since 2017 made considerable efforts to detect and report suspected offences to the FIU.

Luxembourg has put in place a strong legal and regulatory framework to combat international tax evasion. The Organisation for Economic Co-operation and Development's (OECD) Common Reporting Standard (CRS) for the automatic exchange of financial information was implemented in 2017. The OECD has rated Luxembourg to be "fully compliant", with the legal framework being "in place" and the effectiveness "on track"".[58] Luxembourg is also a Member of the OECD/G20 Inclusive Framework on BEPS (Base Erosion and Profit Shifting) and has approved the *July 2023 Outcome Statement on the Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy*, which will ensure multinational enterprises are subject to a 15% minimum corporate tax.[59]

4.2.2. Fraud

Fraud in this section refers to a broad set of deceptive practices.

Globally, private banks can be abused or misused to launder the proceeds of various types of fraudulent activity. These can range from simplistic frauds such as falsification, to more complex schemes, such as:

Ponzi schemes: investment schemes in which money from new investors is used to provide a return/repayment to previous investors.

Insider Trading:[60] an individual or group trade on the stock exchange to their own advantage through having access to confidential information.

Advance fee fraud: a criminal offers a high reward in exchange for a fee to be paid in advance. Once the fee is paid, the criminal disappears.

Forged invoices: E.g. invoices sent via electronic communication means are intercepted, the invoice details and payment account are modified, then the forged instructions are transmitted onwards to the recipient with a label "urgent". An accompanying telephone call will highlight the urgency and leave the false impression of a verbal confirmation.

Cyber Fraud: In particular, via phishing, which is a form of social engineering and scam where attackers deceive people into revealing sensitive information or installing malware

[57] "Traditional banks" designates banks that do not operate exclusively online.
[58] OECD Global Forum on Transparency and Exchange of Information for Tax Purposes, *Peer reviews of the AEOI Standard's implementation | READ online (oecd-ilibrary.org)*, 2022
[59] OECD, *138 countries and jurisdictions agree historic milestone to implement global tax deal*
[60] In Luxembourg's NRA, 'Insider Trading' is treated as a separate category of predicate offence. Here it is grouped alongside 'Fraud and Forgery' in the broad category of 'Fraud'.

such as ransomware[61]. Phishing has become increasingly common via electronic communication means and platforms as a way to commit (online) fraud.

CSSF has over the past decade also noted a consistently high number of fraud attempts over the internet by entities pretending to be licensed financial intermediaries or misusing the names of licensed financial intermediaries. These schemes involve criminals trying to attract customers through an interesting offer of investment services by reference to Luxembourg's reputation as an international financial centre.

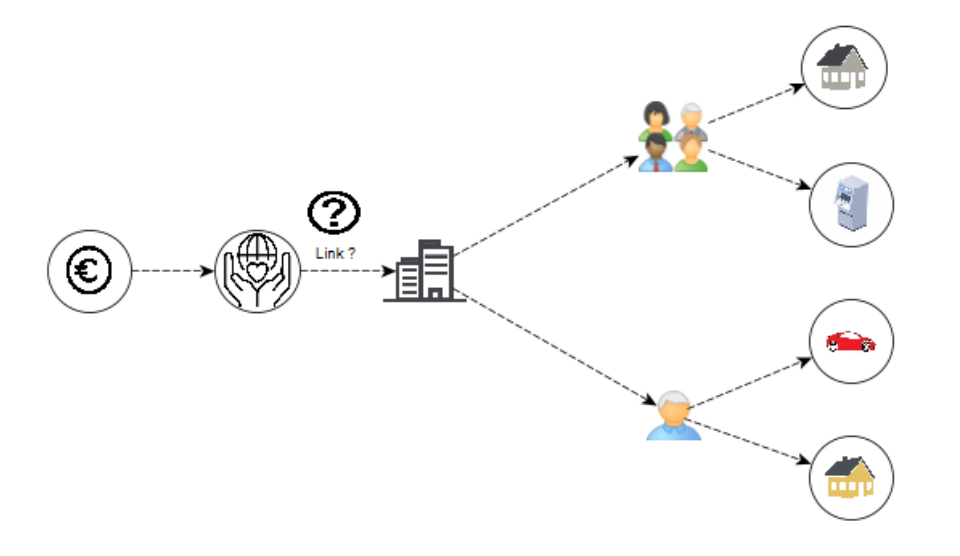
Figure 6: Case study: Abuse of corporate assets[62]

The following case study describes a technique of abuse of corporate assets involving a non-profit organisation (NPO), a commercial company (Company) and the private bank accounts of the Company's ultimate beneficial owner (UBO).

More specifically, suspicious transactions can be observed between the NPO paying substantial sums to the UBO's personal bank accounts, as well as to the Company's corporate bank account. The funds received from the NPO are the Company's sole source of income. Moreover, no apparent link exists between the NPO's activity and the Company's official business purpose.

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

The inflows observed on the NPO's bank account are exclusively donations paid in from foreign debit cards and allegedly relating to donations made for sick children. No outgoing transactions in connection with the fulfilment of the NPO's purpose have been identified.



Red flags:

- No online presence, website nor official listing of the NPO
- Suspicious transactions between the UBO's account, the Company and the NPO
- No outgoing transactions in line with the NPO's purpose

[61] Source: Wikipedia
[62] Case study provided by the CRF

- No incoming and outgoing transactions in line with the Company's business purpose

Figure 7: The COVID-19 crisis

The COVID-19 crisis has given rise to specific fraud typologies. Criminals have tried in particular to exploit shortages of certain medical supplies to artificially inflate prices, deliver counterfeit products, obtain advance payment for products that were never delivered. Furthermore, the hurried transition to remote working and increased reliance on electronic communication have presented opportunities to bypass traditional fraud controls.

According to the CRF, in 2020 COVID-19 related fraud attempts were mainly reported by online payment service providers[63]. Fraud related to medical supplies was dominant and almost exclusively occurred during the first months of the crisis. This appears logical insofar as medical masks, disinfectants or test equipment were particularly scarce or inexistent in winter/spring of 2020 while at the same time seasonal effects increased the virus' impact.

In similar crisis situations, private banks, too, could inadvertently become involved in a fraudulent scheme driven e.g. by a new client whom they do not know very well yet. Any crisis situation typically implies the use of emergency measures and processes that deviate from established procedures and offer opportunities to criminals to bypass traditional, well-proven controls. Identifying a new client or the legitimate sender of an instruction can become more difficult. Private banks should draw conclusions from potential difficulties encountered during the COVID-19 crisis and ensure their crisis procedures incorporate mechanisms to compensate potential weaknesses.

STR/SAR reporting over the years as well as CSSF supervisory experience show that fraud is a material ML threat for private banks in Luxembourg. Accordingly, fraud is not solely driven by predicate offences committed abroad. Furthermore, the international exposure and geographically diverse client base of private banks, the complexity and opacity of some products (e.g. wealth structuring activities) as well as the use of third parties and intermediaries are all factors which can create distance between the private bank and its clients and increase the difficulty for the bank to assess the legitimacy of the client and his business. Moreover, private banks are also exposed to internal fraud, e.g. by account managers exploiting internal control loopholes and falsifying client instructions or transaction records. When combined, all the abovementioned factors create opportunities for criminals to commit fraud in a private banking environment, and then launder the proceeds of these illicit activities through the bank and the financial system.

4.2.3. Corruption and bribery

Corruption and bribery includes all relevant offences defined across Luxembourg's Criminal Code, including domestic bribery (Articles 240 and 310 et seq.) and corruption of foreign public officials as defined in Article 252.[64] Corruption and bribery undermines the rule of law and is often linked to political instability and human rights abuses.

According to the UN Development Programme, of the approximately USD 13 trillion that governments spend on public spending, up to 25 percent is lost to corruption.[65]

[63] CRF, *Annual Report 2020*, 2021
[64] Luxembourg, *Code pénal* (Note, the Luxembourg Criminal Code does not establish quantitative or qualitative limitations on facilitation payments. The analysis regarding a qualification as bribery is made on a case-by-case basis).
[65] UN Development Programme, *The cost of corruption*, 2022

In Luxembourg, the primary exposure of private banks relates to *foreign c*orruption and bribery. This is due to the limited size of the country and the domestic market, the international nature of the sub-sector's activity, the concentration of wealthy and politically exposed clients, and the involvement of third parties and intermediaries. According to the CRF, "declarations received by the CRF often relate to primary offences committed abroad".[66] Although much more limited, private banks should remain watchful also in their domestic relationships. The nature of these exposures is exemplified in the case studies below.

Figure 8: Case study: Money laundering in Luxembourg of a predicate offence committed abroad[67]

This case study is based on allegations of embezzlement of public funds, illicit enrichment and money laundering related to a foreign PEP and beneficial owner of several holding companies under Luxembourg law holding, together with family members and close associates, business relationships with several local banks. Most of the funds held on the accounts in Luxembourg were initially transferred from foreign bank accounts, either private accounts or corporate accounts of offshore companies belonging to the group of suspects, and invested in real estate properties around the world.

A contract suspected to be without economic reality permitted the arrival of several million USD on European accounts of a company, whose beneficial owner was a family member. The funds were then allegedly channelled to other accounts in Europe, then to accounts in non-EU jurisdictions and back to European bank accounts of companies linked to the beneficial owner and his entourage.

The Luxembourgish bank accounts were mainly used as transit accounts shifting funds from nominative or corporate bank accounts held in foreign jurisdictions to further bank accounts opened in other foreign jurisdictions. The purposes of the transfers were mainly in relation with advanced payments or loans provided to companies of the group.

Red flags:

- Pass-through accounts
- The subject in the transaction was a foreign PEP, family members or close associates and received and/or sent unusually large amounts of funds in different currencies
- Funds received in bank accounts of persons, legal entities, or legal arrangements with no visible connection to PEPs, or other officials, but known to be controlled by such (via frontman, strawman)
- Misrepresentation and/or inconsistency (with client profile and/or source of revenues) between the declared source of wealth of a PEP, his/her family members or close associates
- A transaction or financial activity, which involves foreign nationals with no relevant link to the country where the transactions took place
- Financial flows, which reveal complex financial mechanisms and involvement of multiple layers of foreign legal entities or arrangements
- Open-source information relating to ongoing investigations into individuals and concerns about corruption.

[66] CRF, *Annual activity reports.* Applies to all sectors and all declarations.
[67] Case study provided by the CRF

Figure 9: CSSF thematic review: Suspicious transactions involving the Estonian branch of Danske Bank A/S [68]

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/TF risks from its international clientele and the high volume and frequency of cross-border flows.

Findings and Conclusions:

As an international financial centre with a high degree of expertise as well as political and economic stability, Luxembourg is attractive for wealthier clients aiming to protect their assets. CSSF's work has shown that this applies in particular also to high-risk clients from jurisdictions lacking those qualities, but that are known e.g. for a high degree of corruption. These wealthy, high 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 (as well as all other banks) must operate under a clearly defined ML/TF risk appetite, ensure their risk-based approach considers all relevant risk factors and weighs them appropriately (in particular those inherent to clients and geographical origin of assets). Undervaluing client risk typically leads to insufficient due diligence and monitoring measures being applied, exposing the bank to financial sanctions and reputation risk.

The threat from corruption of *domestic* origin is deemed to be comparatively low in Luxembourg.[69] Transparency International ranks the country 10th out of 180 in its Corruption Perception Index (although the country's rank and score have slightly dropped in 2022 as compared to previous years), and the World Bank ranks Luxembourg 9th in its Controls of Corruption Estimate.[70,71]

Overall, when looking solely at STR/SAR reporting over the years, the threat from corruption would appear to be lower for private banks than the threats driven by tax offences or fraud. According to the CRF however, while sometimes all money laundering indicators point to corruption, it can be difficult to prove the link with the underlying primary offence and the declaration could be classified by the CRF as "money laundering" or "other"[72], while nevertheless the laundering of corruption monies remains a very real threat for Luxembourg. The amounts involved in foreign corruption can be important, just as the publicity received by those cases and the reputational damage they create. Also, foreign predicate offences increase detection and verification difficulties because of the

[68] CSSF thematic work, 2019
[69] NRA, 2018
[70] Transparency International, *Corruption Perception Index*, 2022
[71] World Bank, *Data Bank: Worldwide Governance Indicators, Control of Corruption*, 2021
[72] CRF, *Annual activity report 2021-2022,* 2023

dependency of information from sometimes remote countries and foreign press articles, therefore private banks should remain cautious and readily declare suspicions to the CRF.

4.3. TF threats in private banking

4.3.1. Situation in the European Union

Terrorist financing refers to the financing of terrorism, terrorist acts, terrorists and terrorist organisations. It encompasses the raising, movement and use of funds by terrorist actors or terrorism sponsors and financiers and is considered as one of the most important threats to global security.[73]

The SNRA continues to assess TF risk in the private banking sector as non-relevant. However, it admits the possibility that wealthy terrorism sponsors might use private banking services in the EU to manage on their behalf assets not directly related to, or intended for, the financing of any terrorist activities[74].

Table 5: SNRA analysis of ML/TF risk in private banking, 2017 - 2022

SECTOR/PRODUCT	2017		2019		2022	
	TF residual risk	*ML residual risk*	*TF residual risk (shift)*	*ML residual risk (shift)*	*TF residual risk (shift)*	*ML residual risk (shift)*
4. Private banking sector	0,00	3,00	0,00	4,00 (+1)	0,00	3,50 (-0,50)

Statistics on the number of terrorist attacks that were prevented or failed, as well as arrests linked to terrorism financing compiled by Europol[75] show a declining trend since 2019, with Islamist terrorism remaining a more likely threat for EU Member States than right- or left-wing terrorism. Out of a total of 388 terrorism related arrests reported by Member States in 2021, only 14 were made in relation to the financing of terrorism[76]. Across the EU, individual donations remain one of the primary means of funding for terrorist and violent extremist organisations, and Non-Profit Organisations (NPOs) and charitable organisations continue to be used by terrorist organisations and sponsors to obtain donations. Although crowdfunding and online payment and money value transfer services seem to attract a growing interest, the traditional banking system and smurfing techniques remain a frequent choice for transferring funds across borders.

4.3.2. TF exposure of private banking in Luxembourg

Luxembourg private banks' potential exposure is driven by the relative importance of the sector, its international nature and clientele as well as the general banking ability to facilitate rapid cross-border flows of large sums of money.

In line with the NRA, the most relevant risk driver for the banking sector as a whole is the cross-border movement of funds. Terrorist actors could misuse/abuse banking products

[73] FATF, *International standards on combating money laundering and the financing of terrorism and proliferation – the FATF recommendations*, 2012
[74] European Commission, *Commission staff working document accompanying the REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, 2022
[75] Europol, *European Union Terrorism Situation and Trend Report 2022*, 2022
[76] Europol, *European Union Terrorism Situation and Trend Report 2022*, 2022

and services, for example by opening a current account and using the associated debit card to withdraw funds oversees (e.g. in a conflict zone or where an attack is planned). The low value nature of such activity makes it difficult to detect, with research showing that 75% of violent extremism cases in Europe between 1994 and 2013 cost less than USD 10,000.[77] The limited cost of terrorism acts makes retail and online banks more suitable to be misused for this purpose.

In private banks, the close relationship between the client and the bank, the high entry thresholds, the longer-term view on investments, the particularly high level of due diligence and the specific nature of transactions (high value, but low numbers facilitate a closer scrutiny) make them an unlikely and unsuited target for the financing of (low value) terrorist support or acts. Luxembourg private banks also have a traditional operating model, preferring direct contact and face-to-face relationship management over solely online identification and communication methods.

In accordance with the SNRA, Luxembourg private banks could in theory be exposed to TF risk driven by wealthy individuals or organisations that act as terrorism sponsors or are suspected to support terrorist organisations, and who invest money not directly linked to, or directed at, the financing of terrorism, via their accounts held with a private bank.

This risk could be particularly high with clients such as legal entities or arrangements, or even NPOs, where beneficial ownership and the exact nature and purpose of their activity can be more difficult to establish.

An initial review of the financial flows of Luxembourg private banks with jurisdictions presenting a higher potential risk of involvement in terrorist financing has not shown any obvious exposure. This has likely to do with banks' awareness of TF risk and their Europe-centric client base. The share of clients from across Europe and in particular the EU, has over the past years represented over 80% of the sub-sector's total client base, while the share of client relationships originating from jurisdictions considered high risk for the purpose of ML/TF has consistently remained below 0.5%.[78]

In a second phase, CSSF has now launched a more focussed, risk-based analysis of selected banks and flows across all sub-sectors, to achieve a more granular assessment of any potential TF threats.

CSSF's supervision, rigorous market access controls and preventive as well as repressive measures have done their part to minimise risk. The fines imposed by CSSF on banks over the past years, many of which were related to CDD deficiencies, have resulted in banks enhancing their CDD processes further, especially the initial due diligence and risk assessment for higher risk clients. Discussions at the EWG PB show that private banks are today very aware of the risk represented by their increasingly HNW/UHNW client base.

Other elements explaining the absence of a material exposure to TF in private banking in Luxembourg, are the products offered and the nature of private banking transactions. Private banks in Luxembourg do currently not offer virtual assets or similar high-risk products. The preferred service offered by private banks is portfolio management. Discretionary portfolio management brings the clients' assets under control of the bank, in line with a signed mandate, so that the clients cannot dispose freely themselves of their assets under management with the bank.

As regards cross-border transactions, while transaction sizes in private banking are large, owing also to the increasing share of HNW/UHNW clients, the number of transactions is much lower than in retail banking, enabling private banks to perform more intrusive investigations on the origin and destination of fund flows during the in- and outflow phases.

In light of the preceding, the type of banking activities most exposed to TF risk would be those of online banks, as well as retail and business banks, rather than private banks. CRF

[77] Forsvarets Forskningsinstitutt, Oftedal, Emilie, *The financing of jihadi terrorist cells in Europe*, 2015
[78] CSSF & ABBL data, 2021 & 2022

statistics and conclusions indeed show that the vast majority of TF related declarations are made by the online and non-bank sectors. As regards traditional banks, while the number of TF related declarations has generally declined in recent years, it is retail and business banks that file most declarations, whereas the number of declarations made by private banks is almost non-existent.[79] This picture is aligned with the general assessment that private banks' exposure is not exposed to terrorism financing transactions, but rather to wealthy terrorism sponsors that might invest their assets not directly related to terrorism with private banks.[80] Hence, private banks' detection of TF-linked transactions will be limited and their efforts focussed more on carrying out strong due diligence, monitoring sanctions and black lists, and screening the media for the names of their clients. Therefore also, any declarations based on those screening results should not be considered pure defensive reporting.

The CRF received a total of 454 TF related declarations in 2020, 321 in 2021 and 220 in 2022 (TFAR and TFTR combined). Within the above totals, traditional banks generated 40 declarations in 2020 (5 by private banks), 15 in 2021 (none by private banks) and 10 in 2022 (only 1 by a private bank).[81] While the number of yearly declarations appears to be decreasing, as also identified by Europol, it remains to be seen if this trend will continue through 2023 and 2024 in light of more recent geopolitical instability and armed conflicts.

As a conclusion, while there is today no strong indication that private banks in Luxembourg are particularly exposed to TF risk, they are well advised to remain cautious and continue monitoring not only sanctions lists, but also other public "black" lists as well as negative press closely, as these are key sources for their TF prevention.

Figure 10: Case study: Luxembourg banks' exposure to terrorism financing [82]

A suspicious wire transfer from a Luxembourgish bank account held by a foreign citizen to a non-EU country account was reported to the CRF.

The suspicions were mainly based on press articles related to raids in an EU Member State targeting two NPOs. The NPOs were suspected of aiding a religiously motivated terrorist group under the guise of humanitarian aid. As a result of these press articles, the reporting entity had placed the bank accounts belonging to those NPOs on an internal "blacklist".

It turned out that the beneficiary account of the above-mentioned wire transfer matched one of the blacklisted bank accounts.

[79] CRF, *Annual Report 2021-2022*, 2023
[80] See also SNRA and Luxembourg's Vertical risk assessment on terrorist financing, published in 2022: https://mj.gouvernement.lu/en/dossiers/2020/lutte-blanchiment/evr.html.
[81] CRF, *Annual Reports 2020* and *2021-2022*, 2023
[82] Case study provided by the CRF

5. INHERENT RISK – VULNERABILITY ASSESSMENT

This chapter evaluates how vulnerable the core and ancillary activities of private banking identified in Section 3.1 are to ML risks. Overall, the activities of the sub-sector are considered **inherently high risk**.[83]

Table 6: Summary of ML/TF inherent risk – vulnerability assessment

Sub-sector	Inherent Risk	Activities		Inherent Risk
Private Banking	High	Asset management	Custody of financial assets	High
			Investment services	Medium-High
		Ancillary services	Current account banking	High
			Credit solutions	High
			Wealth structuring	High
			Insurance solutions	Medium-High

The vulnerability assessment considers five **risk factors**: (1) Clients and geography; (2) Intermediaries; (3) Market structure; (4) Activities and products; and (5) External advisors, and analyses how these five risk factors influence the ML/TF risk in the two core and six ancillary activity categories.

5.1. Risk factors impacting private banking activities in Luxembourg

5.1.1. Clients and geography

Risks linked to 'clients and geography' impact all private banking activities. The large client base (in excess of 150,000 accounts according to ABBL) and the increasing share of more sophisticated HNW/UHNW clients also increase the ML risk of private banking in Luxembourg. According to the ABBL, UHNW clients with AuM exceeding EUR 20 million represented in 2022 close to 60% of all private banking AuM in Luxembourg, whereas in 2011 this client category represented 41% only. At the other end of the spectrum, affluent clients with AuM of less than EUR 1 million saw their share decrease from 24% to only 7% in 2022. While affluent clients still represent the majority of private banking clients in number, they hold a minority of total AuM in Luxembourg.[84]

A non-negligible (albeit decreasing) share of private banking clients in Luxembourg are legal persons or legal arrangements. The use of more complex, international ownership structures (e.g. to facilitate investing or wealth structuring and ensure privacy to especially

[83] Note, this risk assessment uses a four-point scale (High, Medium-High, Medium-Low, Low) compared to the five-point scale used in the NRA (Very High, High, Medium, Low, Very Low). The conclusions of this risk assessment and the NRA are therefore in line.
[84] ABBL & CSSF data, 2013-2022

HNW/UHNW clients) can also decrease transparency regarding beneficial ownership. Multiple corporate layers or legal structures that potentially obfuscate beneficial ownership can increase ML/TF risks for private banks as they may have difficulty in ensuring full visibility on beneficial ownership.

In terms of geographical origin, according to the KPMG-ABBL survey and CSSF internal data, the majority of AuM belongs to clients from Europe, but outside Luxembourg. This may complicate the identification of beneficial owners and the origin of their wealth. Approximately one fifth of private banking AuM belong to Luxembourg accountholders.[85,] The diverse, international clientele reflects the attractiveness of Luxembourg as an international private banking centre, but it can also decrease the level of transparency on the funds invested in the sub-sector.

Private banks themselves rate a considerable share of their clients high ML/TF risk. The percentage of clients rated high risk is higher than in other banking sub-sectors and represents about 20%.[86]

Clients that are residents of high risk or non-CRS participating jurisdictions, or whose wealth originates in high-risk jurisdictions or high-risk industries, can increase ML/TF risk (e.g. as concerns tax crimes or corruption) for the bank. While the number of those clients is very low, their impact on the sub-sector's reputation can be disproportionate.

CSSF's analysis and supervisory experience, including from onsite inspections, shows that the 'clients and geography' category represents the most important risk driver in private banking. This conclusion comes hardly as a surprise: private banks' clients largely determine the ML/TF risk, through their past and current activities and actions, the source and origin of their wealth, their business relationships and affiliations. Accordingly, it's on initial and ongoing due diligence that banks need to focus to a large extent their AML/CFT compliance efforts.

5.1.2. Intermediaries

A number of banks use intermediaries in providing private banking activities. This assessment identifies 3 sub-categories of intermediaries used by private banks and their clients: business introducers, 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 and hence complicate initial as well as ongoing due diligence. Transparency on beneficial ownership or source of wealth can be reduced and therefore exposure to threats such as tax crimes, corruption or fraud may increase.

Business introducers help private banks acquire new clients and grow their AuM. They can be licensed or registered professionals (such as tied agents), supervised for AML/CFT purposes, be part of the same group, and/or bound by a commercial agreement. Approximately 15% of private banks are working with business introducers who assist the bank in performing CDD obligations[87]. As a result of this intermediation between private banks and their clients, level of transparency and direct interaction with clients and beneficial owners may decrease, potentially reducing banks' knowledge about their clients.

Similarly, the presence of POA-holders with signatory authority over a client's account and acting on behalf of the client may limit the direct contact between the client and the bank, making it more difficult to "know the client" or understand his/her transactional account behaviour. POA-holders may be from any jurisdiction and there are no mandatory

[85] KPMG-ABBL, *Clarity on performance of Luxembourg private banks,* 2023
[86] CSSF internal data, 2022
[87] CSSF internal data, 2021

requirements of supervision or registration, nor even professional qualifications, which may further increase risk.

Third-party managers act on behalf of their clients. Their clients' assets may be held in an omnibus account with the bank, where the bank has a limited relationship with the third-party manager's clients. The bank may perform certain contractual tasks on behalf of the third-party manager in accordance with a bi- or tripartite agreement, and must comply with its own legal obligations, e.g. in relation to sanctions lists screening and transaction monitoring. Sometimes clients may agree to move assets to an account in their name at a particular private bank on condition that these assets will continue to be managed, in part or in whole, by a dedicated external asset manager. In this latter case, the bank has a direct relationship with the client. The presence of a third-party manager limits face-to-face interactions between the private bank and its client and may reduce the bank's knowledge of the client, his global investment strategy, portfolio of investments, history of business activities and transactions.

On the other hand, since third-party managers are authorised and supervised, they may provide an additional level of ML/TF control (as they will have their own AML/CFT obligations in respect to their clients).

5.1.3. Market structure

According to the KPMG-ABBL survey "Clarity on performance of Luxembourg private banks", the private banking sub-sector in Luxembourg accounted for EUR 585 billion AuM at the end of 2022.[88,89]

Private banks in Luxembourg have a wide variety of sizes and business models. Not all of them are solely focused on private banking, many banks have a mixed service offer. Most banks offering private banking services are part of, and can count on the support of, European or international groups. There are some large actors, but also a (decreasing) number of smaller institutions competing for a share of the market.[90] Smaller or stand-alone private banks typically have less resources at their disposal, potentially resulting in less sophisticated AML/CFT controls. Not being part of a group means not being able to rely on the group's support, expertise, policies, processes, and international network. The 2022 KPMG-ABBL survey has estimated that, in order to remain economically viable, a private bank must today have a minimum of EUR 10-12 billion in AuM, up from only EUR 5 billion some years back. The study also showed that, as could be expected, larger institutions cope significantly better with rising (regulatory) costs than the smaller ones. This may impact on the risk appetite and exposure of smaller private banks that could be inclined to accept higher risks.

Additionally, smaller private banks may have less sophisticated AML/CFT controls in place (e.g. transaction monitoring systems) than their larger peers, making the monitoring and detection of suspicious account movements initiated by the client (e.g. in relation to bribery and corruption) more difficult.

5.1.4. Products and services

The typical service offer of private banks comprises custody and investment services as well as ancillary products and services relating to current account management and

[88] KPMG-ABBL, *Clarity on performance of Luxembourg private banks,* 2023
[89] Note, private banking can be defined as an activity across all banks, or as the group of those banks offering mainly private banking services. The resulting statistics would differ slightly.
[90] CSSF internal data, 2021

payments, loans and credit lines, life/non-life insurance, wealth structuring and tax and inheritance planning.

Custody services and products inherently have a low exposure to ML/TF, since such services are mostly commoditised and standardised (e.g. custody of shares, dividend and interest payment collection and distribution). However, ML/TF risks may arise due to activity volumes, remote nature of the services, in relation to asset ownership (CDD) or transactions (upon entry/exit of assets).

Investment advisory services include the provision of advice related to more or less standardised investment products available from or through the bank, or schemes that are tailored to the needs of the client. It is difficult to conceal illicit activities through standardised products. However, the vast majority of assets under management in Luxembourg are increasingly held by European HNW/UHNW clients; these clients typically require more complex advisory services and investment solutions (e.g. access to specific corporate and legal structures, alternative/specialised investment funds and/or remote markets) than less wealthy clients with more mainstream investments (e.g. public investment funds with risk diversification requirements such as UCITS).

Discretionary asset management services have a moderate ML/TF exposure, because investments are typically in products that are relatively transparent (e.g. listed stocks and investment funds) and have been reviewed and approved by the bank, who also takes the investment decisions. The bank's investment decisions follow a pre-agreed investment strategy, clients cannot give direct buying orders. Performing and disguising illicit activities within the management mandate is therefore difficult. ML/TF risk is mostly concentrated around in- and outflows, which must be scrutinised by the bank.

Current account and payment services are highly standardised. They are significant in volume and typically allow clients to transact on their own, via electronic banking, which may increase ML/TF risk because of the absence of control by a relationship manager. Although cash withdrawals and deposits still are a common method of ML/TF due to the anonymity provided by cash and the difficulty of monitoring for suspicious activity[91], major cash deposits and withdrawals are today a rare occurrence in Luxembourg private banks.

Electronic payment services are also highly exposed to ML/TF. Whilst private banks are legally obliged, and able to trace the direct recipient/sender of payments, the increasing volume of funds transferred electronically makes illicit funds increasingly difficult to detect.[92] The often cross-border nature of payments further increases risk. Prepaid cards can serve as substitutes for current accounts and facilitate the transportation of cash across borders.

Loans are part of the standard service offer of any bank. They can also be a selling argument to attract new clients and an area for competition among banks. ML/TF risks are typically higher for credit solutions unrelated to (discretionary-managed) investment portfolios at the bank, especially when these loans involve external parties and cross-border business transactions. Credit solutions could for example be obtained by pledging illicit assets as collateral.[93,94] The bank would seize the collateral and sell it if the client defaults on its loan repayment. When credits unrelated to investment services are backed with collaterals from foreign or even offshore jurisdictions, it will become more complex for private banks to assess the origin of funds at the basis of the pledged assets (as detailed in the typology below).

[91] Multiple case studies explain how cash from illicit proceeds may be placed in a bank through cash deposits in the report: FATF, *Money Laundering through the Physical Transportation of Cash,* October 2015
[92] FATF, *Money Laundering using New Payment Methods*, 2010
[93] Note however that all authorised professionals are required by law to obtain all necessary information regarding the origin of the customer's source of funds (see AML/CFT Law, Article 3.2.c and CSSF Regulation 12-02, Article 24).
[94] A collateral is an asset that a lender accepts as a guarantee for a loan. This collateral may be pledged deposits, pledged liquid assets or tangible assets (e.g. a property).

Moreover, clients could use repayment of their loan as a justification to transfer funds of illicit origin deposited in offshore jurisdictions to their accounts in Luxembourg. These funds could be used to repay the principal and interest of the loan.

In contrast, loans granted to improve portfolio returns (e.g. investment lines, margin lending) are less exposed to the above ML/TF risks. Margin lending mostly answers short and medium-term treasury needs linked to a client's strategy for optimising portfolio returns. The risk is particularly low when the portfolio is managed by the bank under a discretionary mandate. The repayment of principal and interest typically derives directly from portfolio returns, and not from an external source of funds. Moreover, the assets in the portfolio typically serve as guarantee for the credit line, often without need for additional collateral.

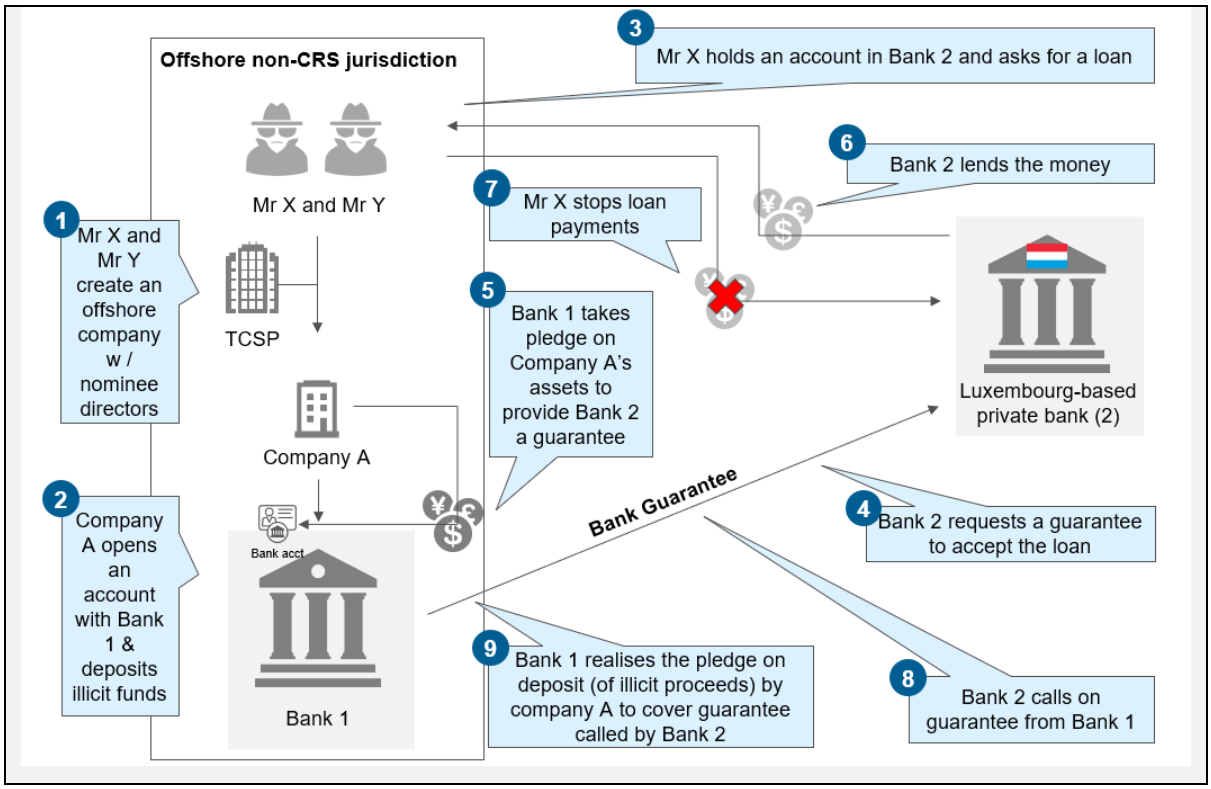
The typology below illustrates how credit solutions unrelated to investment service activities (in this case an international mortgage) could, hypothetically, be abused for laundering illicit proceeds used as collateral.

Figure 11: Typology: Use of a loan & collateral to launder illicit funds

The following example illustrates how credit solutions can be abused or misused to launder collaterals generated from illicit activities. The following steps may occur:

1. Mr X and Mr Y create an offshore company A with nominee directors. Company A is in an offshore jurisdiction[95] with strict bank secrecy which is not a member of the Common Reporting Standard. Mr X and Mr Y (owners of Company A) use a TCSP to manage Company A. Their control over Company A is not disclosed.
2. Company A opens an account with Bank 1 in the offshore jurisdiction and deposits illicit funds into the account.
3. Mr X has an account at a Luxembourg-based private bank (Bank 2). Mr X asks Bank 2 for a new loan to invest in a licit real estate project.
4. Bank 2 is reluctant to provide the loan to Mr X as the value of the assets deposited on his account in Luxembourg is not high enough to grant the loan. Bank 2 requests a guarantee to Mr X.
5. Mr X arranges for Bank 1 (through Company A) to provide a bank guarantee to Bank 2, which could be drawn by Bank 2 on Bank 1 in case of a default on the loan. Bank 1 takes a pledge on company A's deposit. The money deposited in Bank 1 originates from the illicit activities of Mr X and Mr Y. If Bank 2 were to call on the guarantee from Bank 1, Bank 1 would use the deposit pledged by Company A to settle the payment with Bank 2.
6. Bank 2 lends the money to Mr X. Bank 2 only sees Bank 1's guarantee, not the individuals controlling Company A – it is therefore difficult to establish the true origin of the source of funds. Through the loan by Bank 2, Mr X can provide a valid explanation for the money used to finance the real estate investment. Mr X initially makes loan and interest payments to Bank 2 using income from the licit real estate investment.
7. After a few payments, Mr X stops paying the payment of the principal and the interest on the loan; and
8. Based on the loan agreement and the banking terms, Bank 2 calls on the bank guarantee from Bank 1.
9. Bank 1 uses the pledged deposit to settle the payment to Bank 2. Mr X keeps the clean money from the loan. Hence, the pledged deposit is laundered.

[95] Offshore companies "apply to the situation where a company is incorporated in one jurisdiction for persons who are resident in another jurisdiction", FATF, *ML&TF through the real estate sector*, 2007.



Wealth structuring (including tax and inheritance planning) comprises services for advising on the client's global investment strategy and on the most appropriate legal or corporate structure to fit the client's needs for asset protection, succession planning and tax planning. It is especially important to HNW/UHNW clients and includes creating bespoke personalised investment schemes. Wealth structuring is offered by some private banks, but more often involves external advisors.

The complex nature of wealth structuring services significantly increases the vulnerability of these activities to ML/TF. Complex and sometimes opaque wealth structuring products (such as tailor-made vehicles and legal structures) can be used both to conceal the proceeds of crime (e.g. proceeds from bribery and corruption) and to enable economic crimes themselves (e.g. tax crimes). They also can be difficult to assess and monitor from an AML/CFT perspective, for example if beneficial ownership is concealed through layers of legal structures in a bespoke personalised investment scheme.

When a private bank is not providing these services itself, it can still be exposed to related ML/TF risks, because of the client accounts held and the transactions processed. The level of ML/TF risk could even increase for the bank, because not being directly involved in the creation of any structures or schemes can limit a bank's knowledge and understanding of them. On the other hand, this type of services is typically used only by a limited number of HNW/UHNW clients because of the cost involved for counselling services and the creation and maintenance of the underlying structures. Private banks are also well aware of the increased ML/TF risk presented by these clients and their more sophisticated set-ups.

Insurance products are generally less flexible than most other financial services (e.g. loans, payment services) as they often pay out against pre-defined events (e.g. death or accident) and require more specific knowledge than banking services. However, insurance products can be vulnerable to ML/TF risks when they have flexibility of payment, flexibility of investment, ease of access to accumulated funds, negotiability (i.e. can be used as collateral) and anonymity.[96]

[96] NRA, 2020

Private banks are not the issuer of insurance but can act as intermediaries (insurance distributors) when they have been authorised to do so by the supervisory authority of the insurance sector in Luxembourg (CAA).

Non-life insurance solutions are considered to hold a low ML/TF risk. The non-life sub-sector offers standard low-risk products, is smaller and less international than the life insurance sub-sector. [97]

Life insurance products are considered to be the most exposed products of the insurance sector. Known money laundering techniques used include retracting from a contract shortly after its signature and requesting a refund of the premium already paid, payments to/from third parties, paying a large top-up shortly before the end of the policy, cashing out of policies prematurely despite high penalties, or using them as a collateral in a setup similar to Figure 9.

However, life-insurance products are typically structured by licensed insurance companies with whom private banks cooperate and who are subject to AML/CFT obligations (including with regard to CDD) identical to those applicable to banks.

Overall, the vulnerability of Luxembourg's insurance sector is considered to be medium, owing in particular to its considerable size and growth in recent years.[98]

5.1.5. External advisors

In Luxembourg, the amount of wealth structuring services offered by private banks themselves is limited since international and large HNW/UHNW clients often require specialist advice and know-how and use their own advisors. Wealth structuring may also be performed by an affiliate company of the Luxembourg private bank or its parent.

External advisors are typically chosen for their financial, legal or fiscal expertise. The use of advisors may increase complexity of the investment schemes or decrease direct interaction between private banks and their clients and ultimate beneficial owners. For instance, when private banks themselves are not at the origin of the credit schemes, the client's rationale for requesting the loan can become more difficult to assess, reducing the possibility to detect ML/TF. Wealth structuring involves specialists such as TCSPs and legal experts, who set up legal entities or legal arrangements including add-on services such as representation, domiciliation, fiduciary/trustee service or tax strategies, while notaries may help configure real estate investment schemes.

[97] NRA, 2020
[98] NRA, 2020

6. MITIGATING FACTORS AND RESIDUAL RISK ASSESSMENT

The purpose of this section is to identify and assess the mitigating measures in place to reduce ML/TF inherent risk. The section is divided into three sub-sections:

- **Risk mitigation by private banking professionals** can be grouped into four main areas: (1) Internal ML/TF risk assessment and risk appetite; (2) customer due diligence (including ongoing due diligence) and individual risk assessment; (3) cooperation with competent authorities; and (4) internal organisation, governance and controls, suitability, and training.
- **Risk mitigation by CSSF** can also be broadly categorised into four areas: (1) promotion of understanding of ML/TF risks (e.g. via publications and regular communication with the private sector); (2) market entry controls, including licensing, qualifying holding and fit & proper processes and procedures; (3) off- and onsite supervision; and (4) enforcement of compliance with AML/CFT obligations (e.g. administrative measures and fines).
- **Most frequent off- and on-site findings**: Typical weaknesses identified during on- and offsite supervision include insufficient documentation, lack of critical analysis with respect to the plausibility of some transactions or the origin of wealth/funds, and late or no reporting to the FIU.

Whilst new potential threats have emerged since the first PBSSRA published in 2019 and some areas for improvement can still be identified in private sector controls, the combined efforts of CSSF and the private sector have nevertheless allowed private banks to maintain a residual risk level of medium-high.[99,100]

6.1. Risk mitigation by private banking professionals

Private banks' mitigating measures have been grouped hereafter in four main areas: (1) ML/TF risk assessment/risk appetite; (2) customer due diligence and risk assessment; (3) internal organisation, governance, training and fitness and propriety; and (4) cooperation with competent authorities. The nature of these mitigating factors is outlined at a high-level below.[101]

6.1.1. ML/TF risk assessment/risk appetite

All professionals including private banks **are required by law to identify, assess and understand their ML/TF risks**[102] **based on their clearly defined risk appetite**, having considered also relevant conclusions from the EC's SNRA, the NRA, and the PBSSRA. Overall, Luxembourg private banks have implemented risk assessments that are

[99] The NRA considers the private banking sub-sector to be inherently "very high" risk. This is because in the NRA, risks are ranked on a five-point scale (Very High, High, Medium, Low, Very Low). This risk assessment uses a four-point scale (High, Medium-High, Medium-Low, Low) and therefore the "high" inherent risk assessment is compatible with the conclusions of the NRA.
[100] The level of residual risk is determined by reducing the level of inherent risk by an amount commensurate with the strength of mitigating factors. If residual risk and inherent risk are the same, this does not mean that there are no mitigating measures in place (only that mitigating measures do not reduce inherent risk substantially).
[101] The description of mitigating factors reflects observed practice and is not intended to be exhaustive.
[102] Article 4, CSSF Regulation 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing, as amended by CSSF Regulation No 20-05 of 14 August 2020.

appropriate considering their level of exposure and risk appetite. The number of related findings identified during CSSF onsite inspections carried out in 2020-2021 is very low.[103]

6.1.2. Customer due diligence and individual risk assessment

Private banks apply a number of measures to assess and control the individual risk linked to each customer or group of customers. These include the CDD process at onboarding (which often involves an "acceptance committee") and ongoing due diligence throughout the business relationship.

Customer due diligence[104]

When customers are onboarded, private banks **assess the ML/TF risk** and conduct a **due diligence process (CDD)**, applying their risk-based approach. They identify the customer and verify his identity using reliable and valid documents and data from independent sources. They also identify the beneficial owner and obtain information on the purpose and intended nature of the business relationship as well as the source of wealth. This process involves screening against PEPs, sanctions lists and other public information available (e.g. on the internet), as well as typically database information acquired from commercial sources (e.g. WorldCheck). Where ML/TF risks are higher, an **enhanced due diligence (EDD)** with additional verification measures may be performed. Enhanced CDD is legally required in the cases specified in article 3-2 of the AML/CFT Law, including business relationships and transactions with natural and legal persons from higher risk countries as well as PEPs. In certain circumstances (e.g. in relation to PEPs or cross-border correspondent relationships), senior management approval is legally required before establishing the business relationship.

For many private banks, acceptance of new customers also requires written authorisation from a manager or specifically appointed internal body. This ensures decision-making is made by those with appropriate seniority and allows for the intervention of AML/CFT compliance officer(s) where appropriate. In certain cases, a specific acceptance committee provides the authorisation. These committees are composed of individuals from different departments within the organisation (e.g. executive management, sales, legal, compliance) and ensure a range of perspectives are incorporated into decisions to authorise new relationships.

Where third-party professionals are used by private banks to conduct CDD, they **must abide by all the professional obligations** enshrined in the AML/CFT Law.[105] Whilst such third-party professionals can come from outside Luxembourg, private banks are obligated to ensure they meet the conditions prescribed by law, and must not rely on those professionals that are established in third countries and do not (or insufficiently) apply AML/CFT measures. Additionally, any private bank using an external service provider for CDD services must draw up a contract setting out the service provider's detailed obligations and enforce appropriate monitoring of the service provider's compliance, while the responsibility remains entirely with the bank.

The creation in 2019 of a register of beneficial owners of entities registered on the trade and company register, as well as the creation in 2020 of a register of fiducies and trusts recording the settlors, trustees, fiduciaries, protectors, beneficiaries or classes of

[103] CSSF internal data, 2020-2021
[104] Note, this is sometimes referred to as completing "Know Your Customer" (KYC) checks.
[105] The AML/CFT Law defines third parties as professionals (as listed in Article 2), the member organisations or federations of those professionals, or other institutions or persons situated in a Member State or third country that: (a) apply customer due diligence requirements and record-keeping requirements that are consistent with those laid down in this law and in Directive (EU) 2015/849; and (b) have their compliance with the requirements of this law, Directive (EU) 2015/849 or equivalent rules applicable to them, supervised in a manner consistent with Chapter VI, Section 2 of Directive (EU) 2015/849.

beneficiaries and any other natural person exercising effective control over, or benefitting from a trust or fiducie, have provided banks with additional means of corroborating beneficial ownership of legal entities and arrangements, but also created an obligation for them to maintain the register data on their eligible clients and beneficiaries up-to-date.[106]

Ongoing due diligence

In addition to CDD/EDD at onboarding, private banks also conduct **ongoing due diligence** on the business relationship. This includes ensuring that documentation and data collected during CDD/EDD is kept up to date, as well as conducting periodic due diligence on existing client relationships on the basis of materiality and risk (e.g. re-screening new/changed client data against sanctions, PEP and other high-risk lists during periodic and event driven reviews).

Banks also monitor transaction activity and screen accountholders, related parties, beneficiaries and transaction data against various sanctions lists. They keep all necessary records on transactions (both domestic and international), as well as records obtained through CDD measures, account files and business correspondence, and any analysis undertaken in accordance with legal retention requirements.

The due diligence of clients at onboarding and on an ongoing basis is aided by the majority of private banks making use of the "dedicated banker" principle ("*banquier attitré*"). Under this principle, each client has a dedicated relationship manager. The relationship manager's close contact with the customer facilitates understanding the client's source of wealth, why complex or unusual arrangements may nonetheless be genuine and legitimate, or why extra security may be appropriate, improving 1st line controls. However, since this may also give rise to conflicts of interest if the relationship manager is too close to the customer, a solid internal governance and 2nd line oversight are important.

6.1.3. Cooperation with competent authorities

Private banks cooperate with competent authorities through several different channels. These include monitoring transactions and accounts and reporting those that are suspicious to the CRF, as well as participating in and helping to drive forward industry cooperation initiatives such as the EWG PB.

Suspicious activity and transaction reporting

Private banks **monitor transactions undertaken by clients** to ensure those are legitimate and consistent with the banks' knowledge of the customer, their business and risk profile, and known source of funds. This includes the screening of all incoming and outgoing transactions against sanctions, PEPs, and other high-risk lists, as well as the monitoring of transactions to identify potentially suspicious activities, behaviours and transactions. Private banks also ensure that the requirements of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds, are complied with.

According to the EC's 2022 SNRA, the level of suspicious SAR/STR reporting by the private banking sector across the EU remains relatively low, raising the question whether private banks' commercial objectives might conflict with reporting obligations, or whether there is enough awareness in the sector of the threats faced, in particular with regard to fraud and tax evasion.

When private banks suspect, or have reasonable grounds to suspect, that funds are the proceeds of a criminal activity (or are related to TF), they are obligated to report this to

[106] Refer also to section 6.2.3 below.

the CRF. While there naturally are fluctuations in the number of declarations by private banks over the years, private banks' share of the declarations filed by all traditional banks has represented around 33% (one third) each year since 2019, when the initial PBSSRA was published[107].

This figure does not permit the conclusion that private banks in Luxembourg show an unexplainably low level of declarations, hence a low level of ML risk awareness or a high degree of protectiveness towards their clients. In fact, in recent years, the private banking sub-sector has regularly shown a ratio of number of declarations / number of accounts higher than that of other sectors, such as the retail sector.[108] That the absolute number of declarations remains lower than in other sub-sectors is owed to several factors: For one, the number of private banking accounts and the number of private banking transactions is relatively low, although the amount per transaction is typically much higher. Furthermore, private banking usually has restrictive entry criteria and a thorough acceptance process, and private bankers develop a much closer relationship with their clients and a better understanding of their clients' activities and transactions.

In addition, reports with in-depth analyses of the client relationship, even when they are triggered by negative press, are a valuable source of information for the CRF given Luxembourg's exposure to predicate offences committed abroad.

Other forms of cooperation

In addition to fulfilling their obligations in relation to STR/SAR reporting, private banks cooperate with competent authorities through various other channels. For example, banks communicate regularly with CSSF, both on a bilateral basis and through participation in relevant workshops, conferences and AML/CFT colleges. The EWG PB also played an important role in the drafting of this assessment and the understanding of ML/TF risks in Luxembourg in general. In addition, in respect to ML/TF investigations, private banks provide any additional information requested by the CRF or other relevant authorities and make client account data available to competent authorities via a central electronic data retrieval system related to IBAN accounts and safe-deposit boxes established by the Law of 25 March 2020.

6.1.4. Internal organisation, governance, suitability, and training

Private banks have put in place **policies, controls and procedures** to effectively mitigate and manage ML and TF risks, which are based on their board-approved ML/TF risk appetite and ML/TF key risk indicators, all of which are communicated to employees and monitored on a regular basis. These policies and procedures cover e.g. CDD, client risk assessment, transaction monitoring, wire transfers and cash services, correspondent banking, new products and technologies, reliance on third parties, reporting of suspicious transactions or tipping off. They extend to foreign branches and subsidiaries and ensure that employees adhere to the ABBL's code of conduct and AML/CFT policies and procedures. Furthermore, the majority of private banks in Luxembourg are part of groups whose parent institutions are located in jurisdictions with high AML/CFT standards. These institutions therefore implement local AML/CFT programmes that also comply with their group-wide frameworks as applicable and appropriate.

Private banks also adhere to the **ICMA Private Wealth Management Charter of Quality**. This brings together (in a single document) the guiding principles of best practice adopted by the cross-border private banking industry. It is consistent with the relevant legal framework both at the EU and national level and complements principles such as the Wolfsberg Principles on AML or the recommendations of the FATF. The private banking

[107] CRF, *Activity reports*, 2019-2022
[108] CRF and CSSF data

industry has adhered to the Charter since 2012, committing to common standards of quality, compliance and good market practice that are set out in the Charter.

A CSSF circular letter dated 3 December 2012, required all banks and investment firms to stick to the "comply or explain" principle regarding their adhesion to the ICMA Private Wealth Management Charter of Quality.

Private banks have in place **ongoing employee training and awareness-raising programmes** to ensure staff understand ML/TF risks and AML/CFT obligations. Participation in basic (internal and/or external) training is typically required upon hiring and continuing education takes place throughout an individual's career. Holding regular information meetings to ensure employees are kept up to date with the latest trends and developments in ML/TF and preventive measures, and periodically distributing AML/CFT-related documentation is a best practice.[109]

All banks conduct **fit and proper reviews** of management body members and key function holders, to ensure that key positions are filled with people that are suitable and have the required understanding of, i.a., the fight against money laundering and terrorism financing.

In addition to the above, many banks have taken steps to further strengthen **1st and 2nd line controls**. In the 1st line, riskier activities such as cash deposits have in many cases been limited or are not offered at all. In recent years, there has been a significant increase in Compliance headcount/staff per bank. Compliance functions are independent from the 1st line with direct reporting lines to executive management and the Board.

The long history and high degree of maturity of ML/TF prevention in the banking sector also has to be taken into consideration when evaluating its understanding of ML/TF risks.

6.2. Risk mitigation by CSSF

The mitigating measures employed by CSSF are grouped into four main categories, each of which is described below: (1) Understanding of ML/TF risks; (2) Market entry; (3) Supervision; and (4) Enforcement.

6.2.1. Understanding of ML/TF risk

The dedicated AML/CFT offsite division within CSSF's Banking Supervision interacts with supervised entities on a bilateral basis, primarily through their Chief Compliance Officer (CCO) and/or other managers responsible for compliance with AML/CFT professional obligations.[110] Meetings are held on a risk basis. All higher risk banks are met at least once a year. The division also regularly interacts via face-to-face meetings, calls and written correspondence with key senior managers within supervised private banks, e.g. to review the content of CSSF Financial Crime Survey, the outcome of ML/TF risk assessments, as well as to discuss any deficiencies identified during ongoing supervision and to follow up on their remediation. CSSF also interacts regularly with Chief Internal Auditors (CIA) and the external auditors.

Each year since 2017 CSSF's Banking Supervision sends out a survey to banks to collect ML/TF-relevant data enabling it to monitor key indicators for the evolution of sector and sub-sector risk, as well as the implementation, by the private sector, of preventive

[109] For example, private banks may distribute relevant extracts/analysis related to the CRF's Activity Reports, which contain details (e.g. techniques, mechanisms and instruments) on specific cases that gave rise to suspicious transaction reports.

[110] See also definitions of *"compliance officer in charge of the control of compliance with the professional obligations"* and *"person responsible for compliance with the professional obligations"* in CSSF Regulation No 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing, as amended.

measures. This annual data collection exercise enables CSSF to maintain and finetune its understanding of the sector's ML/TF exposure and give focus to its supervision and communication. Banking Supervision's AML/CFT division regularly organises and participates in private sector events and the EWG PB, where it shares information about its understanding and raises awareness of potential ML/TF issues. This allows CSSF to regularly meet business executives and CCO of private banks operating in Luxembourg to exchange on AML/CFT topics (among others) and further strengthen the sub-sector's AML/CFT framework.

CSSF provides guidance to the private sector on AML/CFT obligations and ML/TF risks through regulations, circulars, public statements and appearances, interviews, press releases, monthly newsletters and annual reports. Since 2015, CSSF has published over a dozen circulars on AML/CFT matters applicable to banks, many of which are particularly relevant for private banking actors.

Table 7: CSSF AML/CFT circulars related to banks since 2015

Title	Description	Date	Audience
CIRCULAR CSSF 23/843	Adoption of the guidelines, by the EBA, on money laundering and terrorist financing risk factors when providing access to financial services	October 2023	Credit and financial institutions
CIRCULAR CSSF 23/842	Adoption of the revised guidelines, by the EBA, on money laundering and terrorist financing risk factors – complement of Circular CSSF 21/782	October 2023	Credit and financial institutions
CIRCULAR CSSF 22/822	FATF statements concerning high-risk jurisdictions and jurisdictions under increased monitoring (Annex updated regularly)	October 2022 (updated October 2023)	All supervised entities
CIRCULAR CSSF 21/782	Adoption of the revised EBA guidelines on money laundering and terrorist financing risk factors	September 2021	All supervised entities
CIRCULAR CSSF 20/747	Technical arrangements relating to the application of the Law of 25 March 2020 establishing a central electronic data retrieval system related to IBAN accounts and safe-deposit boxes held by credit institutions in Luxembourg	July 2020	All banks and payments service providers
CIRCULAR CSSF 20/744	Amendment of Circular CSSF 17/650 "Application of the AML/CFT Law" and Grand-ducal Regulation of 1 February 2010 providing details on certain provisions of the AML/CFT Law (AML/CFT GDR) to predicate tax offences"	July 2020	All supervised entities
CIRCULAR CSSF 20/742	Entry into force of the AML/CFT Law and of the Law of 25 March 2020 establishing a central electronic data retrieval system related to IBAN accounts and safe-deposit boxes	May 2020	All supervised entities
CIRCULAR CSSF 20/740	This circular provides guidance on specific AML/CFT implications during the COVID 19 Pandemic	April 2020	All supervised entities
CIRCULAR CSSF 19/732	This circular provides additional clarification on the dentification and verification of the identity of the ultimate beneficial owner(s)	December 2019	All supervised entities
CIRCULAR CSSF 18/702	This circular sensitises private banks to ML/TF risks following the NRA assessment of private banking as a highly risky sector. The document details the threats and current mitigation actions.	December 2018	Private banks

CIRCULAR CSSF 18/684	The circular raises awareness about the 13 February 2018 Law coming into effect and amending the AML/CFT Law, providing details about the regulatory changes at stake.	13 March 2018	All supervised entities
CIRCULAR CSSF 17/661	This circular provides guidance on due diligence guidelines agreed by the EU supervisory authorities for simplified and enhanced client due diligence to better assess ML/TF risks under a risk-based approach.	24 July 2017	All supervised entities
CIRCULAR CSSF 17/650	This circular written jointly with the CRF, provides further guidance to the 2017 fiscal reform law extending money laundering offence to aggravated tax fraud and tax evasion.[111] The 2017 fiscal reform law (LRF) amends the Article 506-1 of the Criminal Code and extends money laundering offence to aggravated tax fraud and tax evasion. The circular also provides a list of indicators to assist the professionals in detecting possible laundering of a predicate tax offence.	17 February 2017	All supervised entities
CIRCULAR CSSF 15/609	This circular details the implications of tax information automatic exchange and AML in tax matters for private banks, following the Luxembourg transposition of the directive 2011/16/EU. This 2011 Directive from the European Council integrates OECD Common Reporting Standard.	27 March 2015	All supervised entities

6.2.2. Market entry

CSSF's Banking Supervision includes a dedicated Authorisations division in charge of the assessment of applications for a bank licence as well as for the acquisition of a qualifying holding (QH). This division conducts the entire assessment of all applications, including the assessment of the business model and proposed activities, the adequacy of staff and resources and the appropriateness of the internal organisation, as well as the propriety of the applicant and the fitness and propriety of designated managers. The AML/CFT offsite division participates in licensing and QH files to assess the level of ML/TF risk based on the business plan presented and allocates a provisional ML/TF risk score, as well as assists the Authorisation division in its assessment of the origin of funds used for the licensing or acquisition project. Both the Authorisations division's assessment, which incorporates, as applicable, the analysis made by the AML/CFT division, and its final recommendation are approved by the CSSF Executive Board.[112]

Credit institutions licensed under Luxembourg law are granted a "universal banking" licence.[113] The authority competent for licensing of banks depends on whether the applicant is a credit institution or a branch of a third country bank.[114] As part of the Single Supervisory Mechanism (SSM) framework, the ECB is the competent authority to license

[111] Aggravated tax fraud and tax evasion within the meaning of i) subparagraphs (5) and (6) of paragraph 396 and of paragraph 397 of the General Tax Law (*Abgabenordnung*) (GTL); ii) the first and second subparagraphs of Article 29 of the Law of 28 January 1948 aiming to ensure the fair and exact collection of registration and inheritance duties, as amended (1948 Law); and iii) aggravated tax fraud and tax evasion within the meaning of Article 80(1) of the Law of 12 February 1979 on value added tax.
[112] All bank licensing and QH applications, except where related to third country branches, are submitted to the ECB for decision.
[113] Luxembourg licensed credit institutions are "all-purpose banks" (universal banking licence) meaning that, based on the licence granted, they can provide any activity of the appendices 1 and 2 of the LFS.
[114] Branches of non-EEA (European Economic Area) parent banks

all new credit institutions within the Eurozone.[115] Nevertheless, CSSF is the entry point for the licensing applications of all new banks in Luxembourg, and is itself the competent authority to license all branches of third country banks in the country.[116] CSSF's market entry controls aim at preventing criminals and their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in financial institutions.

During the licensing or strategic QH processes, AML/CFT policies, fitness and propriety of the owners and proposed management body members, as well as the AML risk level of the future (or target) bank are systematically assessed. In case the resulting ML/TF risk profile of the future (or target) bank cannot be adequately mitigated via the imposition of conditions, the application process is stopped.

6.2.3. Supervision

CSSF's supervision of private banks spans both offsite and onsite activities. AML/CFT obligations of supervised professionals are defined in Luxembourg law and regulations, including CSSF regulations. CSSF provides interpretation and guidance on the application of the law (e.g. via circulars or FAQ's) and requests any relevant information (e.g. via ad hoc requests or the annual Financial Crime Survey).

In line with a risk-based approach, CSSF offsite supervision conducts desk-based risk assessments at sector[117], sub-sector and entity level.[118] CSSF also meets annually with the CCOs of banks on a risk basis and has frequent written and oral exchanges about topics arising during day-to-day supervision. To perform offsite supervision of banks, CSSF draws on a number of reports received from banks, such as the AML/compliance and internal audit reports, as well as the dedicated AML/CFT report and management letter established by banks' independent external auditors.[119] Offsite supervision also considers the data on risk and mitigation provided by banks in their responses to the annual Financial Crime Survey and the results of the desk-based reviews performed on a risk-basis for instance on the AML/CFT risk assessment, AML/CFT risk appetite, AML/CFT policies and procedures or AML/CFT controls monitoring plans of the banks. The information from these various sources is combined into a solid understanding of each bank's ML/TF risks and the effectiveness of its mitigation measures and a holistic view of the sector/sub-sector.

AML/CFT onsite inspections are performed by a dedicated department, acting on risk-sensitive proposals made by offsite supervision. These inspections' frequency and intrusiveness have increased in recent years. A dedicated AML/CFT onsite inspection division exists within the onsite department since 2012. On-site inspections stand as the most intrusive of CSSF supervisory activities, involving important resources during an extended period (as determined by the scope of inspection). On-site inspections can be full scope (covering all supervisory themes), targeted scope (covering selected supervisory themes) or thematic (covering selected supervisory themes across multiple entities).

Moreover, CSSF closely collaborates and exchanges information with foreign AML/CFT competent authorities, either bilaterally, during multilateral AML/CFT college meetings, or via other dedicated (e.g. ECB) channels, on a scheduled as well as an ad hoc basis, by timely responding to requests and by allowing foreign supervisors to perform onsite inspections at Luxembourg subsidiaries.

[115] Articles 4(1)(a) of the Council Regulation (EU) No 1024/2013 of 15 October 2013. The SSM includes Eurozone members as well as participating countries outside of the Eurozone.
[116] Articles 32 and 32-1 of the LFS
[117] The sector-level assessment is reflected as a CSSF contribution in the bi-annually published NRA.
[118] For further details on ML/TF risk assessments performed at CSSF, please refer to CSSF ML/TF Risk Assessment policy.
[119] CSSF Regulation N° 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing

Over the past years, a number of tools were implemented to assist authorities and private banks when trying to determine beneficial ownership:

The Law of 13 January 2019 established a beneficial ownership register of the entities registered on the Trade and Company Register, improving transparency over those persons with a significant and/or controlling interest in Luxembourg corporate vehicles.[120] Following a ruling of the CJEU, this register, which was previously accessible to everyone, remains accessible to competent authorities and professionals within the meaning of Article 2 of the AML/CFT Law that have signed an agreement with the administrator of the registry.

Furthermore, the Law of 10 July 2020 establishing a register of fiducies and trusts requires the registration of settlors, trustees, fiduciaries, protectors, beneficiaries or classes of beneficiaries and any other natural person exercising effective control over the trust or fiducie.

These registers jointly ensure transparency of beneficial ownership and are accessible to professionals with a legitimate interest.

Finally, the Law of 25 March 2020 established a central search platform for IBAN accounts and safe deposit boxes in Luxembourg, accessible by competent authorities and self-regulatory bodies for legitimate purposes linked to their legal obligations.

6.2.4. Rules enforcement

CSSF has the power to sanction supervised entities for non-compliance with applicable AML/CFT regulations.[121] A wide range of remediation and enforcement measures can be triggered by on- and offsite supervision, as described in the table below. Enforcement must follow the *Procédure Administrative Non-Contentieuse* (PANC) process.[122]

Where the sanctioned professional is a credit or financial institution, as defined by Article 1, paragraphs 3 and 3b of the AML/CFT Law, administrative fines imposed by CSSF against the legal person can reach EUR 5 million or 10% of the total annual turnover of the legal person, whereas natural persons can be fined up to EUR 5 million.[123]

Table 8: CSSF remediation and enforcement actions[124]

Measure	Supervisory tool	French translation	Description
Remediation	Observation	*Observation*	Communication to highlight deficiencies and suggested remedial action
	Injunction	*Injonction*	Requirement to take action within specified time, with consequences for non-compliance
Enforcement	Warning	*Avertissement*	Expression of concern about deficiencies
	Reprimand	*Blâme, réprimande*	Serious expression of concern and disapproval about deficiencies
	Administrative fine	*Amende d'ordre administratif*	Financial penalty in form of one-off payment

[120] The register of beneficial owners was set up to implement Article 30 of the 4th Anti-Money Laundering Directive into Luxembourg law.
[121] Law of 23 December 1998 (CSSF Law)
[122] Law of 1 December 1978, Grand Ducal Regulation of 8 June 1979
[123] Article 8-4 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing
[124] Enforcement actions are administrative measures and sanctions as defined in the AML/CFT Law; Injunctions as defined for example in Article 59 of the LFS.

Public statement	*Déclaration publique*	Disclosure of the breach and enforcement action taken
Temporary ban	*Interdiction temporaire*	Restriction or temporary ban from certain activities
Withdrawal or suspension of licence	*Retrait ou suspension d'agrément*	Definite ban from performing activities

In respect of the years 2015-2020, CSSF imposed close to EUR 26.8 million in administrative fines on Luxembourg banks that were triggered by AML/CFT related supervisory findings. The deficiencies identified often concerned initial as well as ongoing due diligence failures, procedural or organisational weaknesses, and were to a large extent linked to private banking activities and clients.[125]

These figures support the SNRA and NRA conclusions that private banking is the banking activity with the highest ML/TF risk level, as well as the fact that this higher risk level also requires increased compliance efforts to avoid economic as well as reputational losses by those banks that are sanctioned, but also by the Luxembourg financial sector and its economy as a whole.

Although private banks' control frameworks have further improved recently, and the number of high-risk findings during onsite inspections has been going down, private banks must remain watchful and ensure that they maintain effective systems and tools, and adequate resources to control ML/TF risks, especially in a difficult economic environment where cost considerations and outsourcing play an increasingly important role.

As is required by law and expected by the FATF, the sanctions and fines imposed by CSSF, on legal as well as natural persons, are published nominatively. Moreover, in line with a recommendation made by the FATF during its 2023 assessment of Luxembourg, these publications will contain even more details on sanctioned failings going forward. The reputational impact on banks, their board members and their authorised managers can thus be very high.

6.3. Most frequent off- and on-site findings

Whilst overall significant mitigation actions are in place, CSSF has identified several weaknesses in private banks' mitigation measures. Along with best practices observed, these are summarised below.

Table 9: Best practices and most frequent findings from off- and on-site supervision

Item	Description
Best practices	• Establishing a **clear AML/CFT risk appetite** statement and **communicating** it throughout the organisation • Promoting a **strict compliance culture** throughout the organisation, especially in the first line of defence • Installing **effective and appropriate technology** to monitor & detect suspicious transactions, including ongoing bad press screening • Ensuring close oversight over branches and subsidiaries • Ensuring **clear allocation of responsibilities** between 1st and 2nd lines of defence

[125] Based on CSSF / public information

	• Providing control functions, especially Compliance, with the necessary **authority, independence, means and management support** • Ensuring an appropriate "**tone from the top**" such that there is direct participation of the management body in the AML/CFT strategy and framework definition, including regular reporting, and management body action in order to timely and effectively enforce compliance with the strategy and framework • Verifying on a regular basis that External Asset Managers with whom the bank has a relationship have an appropriate AML/CFT framework in place
Most common findings	• Internal ML/TF risk assessment is not / no longer adequate with regard to the activities or their development. • **Absence of application of enhanced due diligence measures to customers presenting higher risk factors** (e.g. inadequate analysis and challenge of information in documents gathered for CDD purposes, failure to question the rationale for complex structures, failure to obtain documentation establishing the legitimacy of the source of wealth and source of funds). • **Shortcomings in the review of customer files** entailing the non-identification of business relationships that are especially at risk or showing signs of tax non-compliance; delays in conducting periodic reviews. • **Transaction monitoring issues** related to scenarios that are not risk-appropriate, or technical deficiencies resulting in an absence of alerts. • Incomplete client data encoded in the system used to carry out **name matching controls** or name matching controls not carried out without delay at the publication of international financial sanction lists. • **Failures to meet the obligation to report, or to report without delay**, (i) any ML/TF suspicion to the FIU, and (ii) sanctioned entities to the Ministry of Finance and to freeze the assets. • **Insufficient supporting documentation** for incoming/outgoing transactions and **lack of critical analysis** of the plausibility of some transactions. • **Insufficient involvement of the Compliance function**.

6.4. Residual risk conclusion

Considering the assessment of the sub-sector's inherent risk and the substantial mitigating measures in place, while however also taking into account conclusions from frequent on- and offsite findings and the resulting areas of further improvement for private banks, the sub-sector's current residual risk, after mitigation, is considered to be effectively reduced down to **Medium-High**, as shown in the following tables.

Table 10: Summary of ML/TF residual risk – vulnerability assessment

Sub-sector	Inherent risk		Residual risk
Private Banking	**High**	*Impact of mitigating factors*	**Medium-High**

Table 11: Residual risk of each element of the taxonomy

Activities	Taxonomy elements	Inherent Risk (IR)	Residual risk (RR)
Asset management	Custody of financial assets	High	Medium-High
	Investment services	Medium-High	Medium-Low
Ancillary services	Current account banking	High	Medium-High
	Credit solutions	High	Medium-High
	Wealth structuring	High	Medium-High
	Insurance solutions	Medium-high	Medium-Low

7. EMERGING AND INCREASING AREAS OF RISK

7.1. Ever expanding list of financial sanctions

The massive sanctions introduced by western nations in response to Russia's war against Ukraine have put sanctions risk into focus. Luxembourg has frozen unprecedented amounts of assets, and the list of sanctioned legal and natural persons on EU lists keeps increasing.

The banking sector as a whole is very much at risk due to its international clientele and business relationships. While private banking is particularly exposed because of the nature of its clients, their geographic origin or business activities and political ties, banks in general have to pay attention when transactions and payment flows relate to Russia or Belarus, or any movement of goods with Russia and Belarus.

Monitoring such an extensive list of sanctioned persons, entities and goods can be challenging, and with each addition to the list, the risk of missing out on a particular person or item, or not detecting mechanisms to evade these sanctions[126], is increasing. The CSSF carries out dedicated on- and offsite analyses and supervisory measures with regard to banks' exposure to these sanctions, their monitoring of sanctions lists and their obligation to freeze and notify authorities (Ministry of Finance, copy to CSSF) without delay.

The Financial Sanctions Law introduced in article 506-1 of the Luxembourg Criminal Code a new primary offence relating to breaches of financial sanctions. Apart from the potential criminal consequences of missing out on a sanction imposed in Luxembourg by the United Nations or the EU, there is also a financial risk arising from the differences between the lists published by various western jurisdictions. Especially the banking sector with its international reach and multi-currency activities, must weigh this risk when making payments internationally in foreign currencies, involving persons not legally sanctioned in Luxembourg and the EU, but possibly under sanctions in the jurisdiction that the payment is directed to or transiting through.

Figure 12: Case study: Circumvention of financial restrictive measures[127]

Latest findings show that since Russia's invasion of Ukraine in 2022, and despite additional restrictive measures against Russia, Belarus and its supporters, including travel bans, import and export bans for multiple goods and services, banning correspondent banking relationships, etc., there has been a steady increase of scenarios amounting to circumvention of restrictive measures or attempts to circumvent restrictive measures. One of the key techniques used to circumvent restrictive measures is the threshold technique, which is described in the case study below:

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

[126] Refer to figure 12, CRF case study: Circumvention of financial restrictive measures.
[127] Case study provided by the CRF

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

By an amendment agreement to the prenuptial contract between the ultimate beneficial owner and his spouse, a percentage of his share interest was transferred to his wife.

In addition, a trusted person of the ultimate beneficial owner purchased a percentage of his shares well below their market value via a sale and purchase agreement (SPA) a few days prior to the designation.

The ultimate beneficial owner also stepped down from all management positions in the group of companies.

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

As of today, the deposits remain frozen under the Luxembourg law, as modified, of 19 December 2020 on the implementation of restrictive measures in financial matters.

Red flags:

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

Considering the circumstances of the changes made to the shareholding structure of the companies involved, it cannot be excluded that the companies remain under the control and ownership of said ultimate beneficial owner by more than 50%.

7.2. Outsourcing of AML/CFT tasks

In the wake of the publication and subsequent transposition of the revised EBA Guidelines on outsourcing arrangements[128], CSSF has noticed a considerable increase in the outsourcing of services by banks, including private banks. While this is not an entirely new trend, the transposition via Circular CSSF 22/806 on outsourcing arrangements has set rules applicable to a broad set of entities and their outsourcings.

There are typically two main reasons that drive outsourcing: (i) improving the quality of service (by contracting specialised services and expertise, that are not available internally, from a specialised external provider), and (ii) increasing cost efficiency (by obtaining services at a lower cost than would be possible internally). When applied with the appropriate weighting, both motives are entirely valid. However, considering pressures on profits and the resulting worsening of cost-income ratios of a number of banks, there is a danger that economic aspects will prevail over the assurance of quality and solidity of AML/CFT related controls and information. A condition to any outsourcing of AML/CFT tasks must therefore be that the resulting level of service remains appropriate, respectively improves where it was not appropriate before. **Banks retain the full responsibility for the performance of outsourced services** and are responsible for assessing potential risks prior to any outsourcing, as well as monitoring and ensuring that all processes work and that the level of quality of the service remains appropriate thereafter. Where banks

[128] *EBA/GL/2019/02, Guidelines on outsourcing arrangements*, 2019

fail to enforce these simple principles, CSSF will take appropriate supervisory measures, including imposing fines.

Outsourcing certain AML/CFT related services (or any other services) does not automatically lead to a corresponding reduction in internal resources. Banks will be required to adapt their internal control processes and reallocate some resources away from a direct, internal control, to the effective monitoring of the outsourcing services provider. They also must implement a fall-back solution, to ensure service continuity in case of a service provider's failure.

7.3. New technologies

Another area of potential emerging vulnerability is new technologies. New technologies can affect banks in different ways. Banks can be indirectly exposed to risks arising from new technologies because of their clients (e.g., when these clients are active in virtual asset settlement). Banks can also be directly exposed themselves when they use new technology in their business (e.g. online identification and the use of artificial intelligence (AI) software in ML prevention, such as AI-driven, self-learning activity and transaction monitoring tools). Banks, including private banks, should keep an open mind as regards new and emerging technologies and their usefulness and effectiveness in the area of AML/CFT. However, the goal ultimately remains to ensure compliance with regulatory requirements, effectively manage AML/CFT risks, prevent failures and avoid negative consequences to reputation and financial soundness. New technologies must therefore be thoroughly tested and their effectiveness and proper functioning verified, before, during and after implementation.

In this context, the CSSF also reminds banks of their obligations under article 2-2 (3) of the AML/CFT Law and the New Product Approval Process, which requires them to assess the risk of any new product, service, system, market or client segment prior to its introduction, and the need to involve the compliance function for assessing the ML/TF risk.[129]

7.4. Virtual assets

Whilst the majority of Luxembourg banks have remained cautious towards a direct offering of virtual assets, there are meanwhile a number of products which allow investors to take an indirect exposure to virtual assets, such as funds investing in virtual currencies. A part of the currently very cautious attitude displayed by banks is certainly linked to the significant decline in value of most virtual assets, as well as the frequent news of failures, crashes and hacking of virtual currency issuers and platforms. While the debate rages on whether to fully regulate, or not, virtual assets, banks should be reminded that the VASP activity in Luxembourg is subject to a registration (until the Market in Crypto Asset Regulation (MiCA), which is imposing new requirements, is fully applicable) and is supervised for AML/CFT compliance since 2022.

[129] Refer to the corresponding sub-chapter of CSSF circular 12/552 on central administration, internal governance and risk management.

7.5. Standalone money laundering / Professional money laundering

Professional money launderers (PMLs) act as intermediaries on behalf of criminals, thus enabling these criminals to evade anti-money laundering and counter-terrorist financing safeguards and sanctions [130]

The intervention of PMLs further obfuscates the true criminal origin of funds by inserting a non-related third party with a legitimate public appearance in the chain of transactions, using front companies that are in no way linked to the true beneficial owner of funds. This makes the due diligence even more complex and difficult. PMLs typically work on a fee or commissions basis and be involved in the laundering of larger amounts.

PMLs can be a risk also for private banks, as they could appear to act as a legitimate private banking client, with assets held with the bank over a certain duration, but with a considerable transactional in and out activity.

Figure 13: Cas study: Standalone – professional money laundering[131]

In general, professional money laundering is the provision of money laundering services to third parties in exchange for a commission, fee or another type of remuneration. The following case study describes one of the techniques used in practice by professional money launders to help their clients move and conceal funds.

Initially, recurring transfers of amounts generally not exceeding the EUR 10,000 threshold between two private bank accounts as well as similar transfers to a third individual's bank account held within another bank had been observed. The transfers were either labelled "loan" or "loan between friends". No explanations, nor supporting documents were provided by the individuals to substantiate and or otherwise corroborate these transactions which were not in line with the declared purpose of the accounts.

It turned out that one of the individuals (individual A), a Luxembourg resident, owned a company providing TCSP services in Luxembourg. This TCSP offered mainly domiciliation, accounting and consulting services. Individual A was or purported to be the beneficial owner of different companies registered in Luxembourg and in other jurisdictions, including international offshore centres. Ultimately, financial flows of exceeding several million euros from different companies to individual A's private bank accounts could be identified. Out of these:

- a portion was transferred from his private accounts to his family and connected companies located in another European country;
- another portion was transferred from his private accounts to an unrelated person C, resident in Luxembourg, without any clear connection to individual A and who in turn transferred high amounts to another family in Luxembourg without any economic reason or apparent connection and withdrew a large portion in cash;
- the remaining funds were withdrawn in cash by individual A.

Red flags:

- Unknown/ poorly documented origin of funds
- Frequent transactions of low amounts generally not exceeding EUR 10,000 threshold between unrelated parties

[130] FATF, *Professional Money Laundering*, July 2018
[131] Case study provided by the CRF

- Frequent incoming transactions of low amounts immediately followed by outgoing transactions of similar amounts
- Cash withdrawals of low amounts generally not exceeding EUR 10,000 threshold
- Involvement of different corporate structures incorporated in Luxembourg and in offshore jurisdictions
- Corporate structure changes shortly prior to legislative changes on the common reporting standards

8. AREAS FOR FURTHER ENHANCEMENT

Recommendations specifically targeted towards private banks will contribute to increasing their understanding of ML/TF risks and AML/CFT obligations.

8.1. Recommendations for the private sector

All institutions conducting private banking activities are required to take a proactive approach to mitigating ML/TF risks. They should use this risk assessment to increase their understanding of ML/TF threats and vulnerabilities in private banking in Luxembourg.

In line with AML/CFT Law, regulations and recently published circulars, including CSSF circular 18/702, CSSF has identified a number of key recommendations to private banks.[132] CSSF will monitor adherence to the following recommendations as part of its supervisory activities and has indicated some examples of how private banks may show compliance with them:

Table 12: CSSF recommendations for the private sector

	Recommendations	How banks may show compliance (examples)
1	Implement a clear AML/CFT risk appetite and strategy, in line with the principle of sound and prudent management and aligned with the bank's means in terms of AML/CFT prevention	AML/CFT risk appetite discussed and approved by the Management Body (MB) in a written, detailed document, including the types of clients, geographies, products and services, and the distribution channels the bank wishes to cover (or avoid) and the resources and tools required to properly control the risk. Communicate the risk appetite to all staff and monitor and enforce compliance on an ongoing basis notably through the use of Key Risk Indicators.
2	Engage the MB in the bank's AML/CFT strategy, policies and processes	Detailed board minutes demonstrating engagement with, and understanding of, AML/CFT issues by documenting not only decisions taken but also preceding discussions.
3	Reflect the findings from this report in the internal risk assessments	Internal ML/TF risk assessments that incorporate mechanisms and findings of this sub-sector risk assessment.
4	Promote and enforce a strict compliance risk culture throughout the whole organisation, in particular at the level of the first Line of Defence (LoD)	Tone at the top demonstrated in communication from the MB. Appropriate ML/TF training programmes (including case-studies) and communication channels in place across the institution, including 1st LoD. Documented monitoring of 1st LoD by 2nd LoD.

[132] Refer also to the "best practices" listed in table 9 above.

5	Ensure robust processes are in place to reliably identify Beneficial Ownership and critically appraise the origins of funds/source of wealth[133]	Documented and updated procedure for (i) identifying and monitoring beneficial ownership and (ii) analysing origin of funds/source of wealth, in line with stated risk appetite and ability to perform these verifications effectively.
5	Ensure clients are reviewed regularly in particular clients classified as High Risk	Documented and updated procedure for periodic review of clients with an annual review of high risk clients and a review of other clients within at least 7 years, as well as effective implementation thereof.
6	Ensure that AML/CFT functions and control functions in general within the banks' organisations have the resources proportionate to the risk of the activities and controls required	Level of AML/CFT related Full Time Employee and their experience, technical resources as well as clearly allocated budgets for AML/CFT activities, are all justified and regularly reviewed by MB in light of changes in level of risk/risk appetite.
7	Ensure that AML/CFT and other internal control functions get the necessary management support in conflicting situations	AML/CFT & control functions with appropriate level of authority and effective and well-functioning reporting line to management and the Board
8	When part of Luxembourg-based groups, ensure that foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with Luxembourg and the host country requirements, respectively the more stringent of the two.[134]	AML/CFT measures clearly documented at both group and branch/subsidiary level, with regular evidence that the central AML/CFT functions effectively control the implementation and respect of group wide policies and procedures.
	When part of foreign-based groups, ensure that the Luxembourg branch or subsidiary implement the Luxembourg requirements as well as the policies and procedures of the group, respectively the more stringent of the two.	Local branch procedures are written and adapted from group procedures to account for Luxembourg legal requirements and context, while still integrated in overall group procedures.
9	When outsourcing AML/CFT related tasks in full compliance with existing regulatory requirements, ensure that the bank retains sufficient substance and control resources to carry out proper monitoring of outsourced tasks and the service provider's compliance with Luxembourg AML/CFT requirements. Responsibility for outsourced tasks will always remain with the bank.	Document outsourcing relationship in detailed agreement and SLA, following written analysis (e.g. SWOT analysis) approved by the MB. Document internal procedures for monitoring adequate service execution and escalating exceptions. Implement regular, detailed reporting by the service provider. Carry out and document regular onsite inspections at the service provider's premises to complement offsite monitoring.

[133] See also e.g. The Wolfsberg Group, *Frequently Asked Questions [on] Source of Wealth and Source of Funds [for] Private Banking / Wealth Management, 2020*
[134] FATF, Recommendation 18

10	Collaborate closely with competent authorities to ensure Luxembourg has an effective national AML/CFT framework	Respond promptly and accurately to requests by CSSF, the CRF or the Parquet; take communication initiative when appropriate. Share best practices or provide feedback on publications (e.g. sharing information within and beyond the private banking AML/CFT EWG).
11	Report promptly and with adequate detail suspicious activities and transactions to the CRF	STR reporting mechanisms in line with risk exposure. Suspicious activity/transaction reports are filed without delay but providing all required and useful information of bank's own investigation (quality of information).
12	Implement effective technology solutions that strengthen the AML/CFT framework across key processes such as KYC, and transaction monitoring and reporting	Implement, monitor, calibrate and regularly update AML/CFT technology solutions, including transaction monitoring and sanctions screening systems, so as to ensure reliable detection, swift investigation, effective blocking and, where necessary, notification of authorities without delay.
13	Adjust and enhance AML/CFT mitigating actions in light of emerging trends and evolution of the business, to sustain effectiveness of AML/CFT controls	Systematic assessment of ML/TF risks before launching new products/services, targeting new markets/type of clients, using new distribution channels. Ability to demonstrate resource changes procedural and system related enhancements are implemented without delay in response to changes in risk exposure.

8.2. CSSF initiatives

CSSF has also identified opportunities and defined initiatives to further enhance its approach to supervise AML/CFT activities in private banking. These initiatives are structured around three primary strategic axes, summarised below.

CSSF will further promote understanding of AML/CFT obligations and ML/TF risks by the private sector. CSSF continues to actively support industry in improving their understanding of AML/CFT obligations and ML/TF risks.

CSSF **will continue to develop and finetune its interactions with banks**, on a bilateral and multilateral bases. For this purpose, CSSF will conduct additional analyses of the data collected via the annual Financial Crime Survey as well as the information obtained during offsite and onsite supervision (including interviews with banks) in order to identify areas where its assistance is most useful. CSSF will share conclusions and make recommendations to the private sector.

CSSF is also **enhancing and strengthening the AML/CFT PPP set up with ABBL, private banks and the CRF** by adding dedicated subgroups. Furthermore, representatives from investment firms and CSSF's Investment Firms Supervision are joining this PPP to further extend its reach and impact.

CSSF will further develop its assessment of TF and proliferation financing (PF) risks, in particular as regards international payment flows through the accounts of Luxembourg banks and in light of the current geopolitical context.

Appendix A. Red flag indicators

The tables below detail red flag indicators for three categories of predicate offence that are particularly relevant to private banking in Luxembourg: tax crimes (fiscal offences), corruption and bribery, and fraud. Note, the presence of an indicator does not in itself justify any conclusion that a predicate offence has been committed.

Further useful information on ML/TF red flags and risk indicators can i.a. be found in:

- documents published by the Luxembourg FIU on their website https://justice.public.lu/fr/organisation-justice/crf.html
- multiple documents published by the FATF ton their website, including:
  - Best Practices on Combating the Abuse of Non-Profit Organisations (2023)
  - Risk-based Approach Guidance for the Real Estate Sector (2022)
  - Guidance for a risk-based approach, Securities Sector (2018)
  - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (2020)
  - Updated guidance for a risk-based approach to virtual assets and virtual asset service providers (2021)
  - Terrorist Financing Risk Assessment Guidance (2019)
  - ML through the physical transportation of cash (2015)
  - FATF, Specific Risk Factors in Laundering the Proceeds of Corruption (2012)
- CSSF, Circular CSSF 17/650 (updated 2020)
- EBA, "Risk factor guidelines" (2021, being updated)
- Publications by The Wolfsberg Group, such as
  - The Wolfsberg Group, AML guidance on credit/charge card issuing and merchant acquiring activities (2009)
  - Wolfsberg Anti-bribery and Corruption (ABC) Compliance Programme Guidance (2017)
  - The Wolfsberg Group Frequently Asked Questions (FAQs) on Negative News Screening (2022)

Table 13: Red flag indicators for fiscal offences in private banking (non-exhaustive)[135,136]

Category	Common red flag indicators (non-exhaustive)
Client structure and location	• Client is a legal person or arrangement setup in a jurisdiction that is not subject to AEOI/CRS/FATCA reporting and the entity has no economic, asset or other reality* • Client is a company or uses companies in which a multitude of statutory changes (unexpected and short-term changes) have taken place (e.g. with the purpose of appointing new managers, moving the location of the registered office)* • Client uses companies or legal structures located in a jurisdiction other than the tax residence or place of regular economic or professional interests of the beneficial owners*

[135] CSSF, *Circular CSSF 17/650*, 2020
[136] CRF, *Annual Activity Reports, Typologies*

	• Clients uses a complex set-up without clear economic or patrimonial justification, or which appears designed to conceal information (e.g. trusts from jurisdiction with no requirement to disclose beneficiaries)* • Classification of a company or legal structure as "Active Non-Financial Entity" based on CRS regulations and without the change being justified by the development of the business of the company or legal structure* • Client uses off-the-shelf companies closed down after short existence
Other client characteristics	• Client has moved tax residence from a jurisdiction that is not subject to AEOI/CRS/FATCA reporting to a jurisdiction that is subject to such reporting without notifying the professional, in order, potentially, to escape reporting* • Client has been identified as non-tax compliant in Luxembourg or another jurisdiction • Client / client's company has been subject to negative press in relation with aggressive tax practices
Client interaction and behaviour	• No face-to-face interaction with the client when opening the account • Client refuses any form of contact or communication without a valid reason • Client does not care about lack of return • Requests for assistance or provision of services whose purpose could be to foster circumvention of the customer's tax obligations* • Lack of professional tax advice to support any tax implications of complex structures
Suspicious activities and transactions	• Client transfers funds from a country considered risky from the point of view of tax transparency or resides in a country not subject to the AEOI/CRS/FATCA reporting • Substantial increase, over a short period, of movements on banking account(s) which was (were) until then scarcely active or inactive, without this rise being justified, notably by a verified development of economic or business activities of the customer* • Inconsistency between transactions and business volume/nature* • Frequent and substantial wire transfers from or to geographies without a legitimate commercial purpose or which are considered risky from a tax transparency perspective* • Commercial transaction at a price that is obviously under-estimated, over-estimated, or inconsistent* • Substantial and/or irregular transactions linked to professional activities on personal/private accounts* • Payment or reception of fees to or from foreign companies without business activities or without substance or link between the counterparties and whose purpose seems to be economically unjustified re-invoicing* • Use of so-called back-to-back loans, without valid justification*

	• Withdrawal or deposit of cash that is not justified by the level or nature of the commercial activity or known professional or asset situation* • Receipt of commissions or payments to foreign companies without commercial activity or without substance
Documentation and source of wealth	• Client unwilling to disclose source of wealth or origin of funds • Insufficient explanations regarding the source of large cash withdrawals or receipts • Findings of anomalies in documentation justifying transactions, and notably atypical or unusual transactions (e.g. no VAT number, no invoice number, circular transactions)* • Client refuses to provide tax compliance documentation or information needed for tax reporting, or the presence of indications raising suspicions regarding fiscal non-compliance (e.g. refuse to communicate tax identification number of fiscal address)* • Client cannot confirm that the source of funds has been declared to a tax authority • Documentation on tax compliance leaving room for doubt as it was issued by a person close to the final customer and there being a potential conflict of interests* • Client's organisation structure is not consistent with the documentation on file
Hold mail	• Request to have hardcopy documents retained for a short time only or personal collection with long time spans in between • Hold mail not collected and the client or their beneficial owners have not visited Luxembourg for an extended period • Unjustified refusal of any contact or unjustified request of hold mail and more particularly if the customer is domiciled in a jurisdiction that is not subject to AEOI/CRS/FATCA reporting*

*Denotes red flag detailed in Circular CSSF 17/650 (2020)

Table 14: Red flag indicators for corruption/bribery in private banking (non-exhaustive)[137, 138, 139]

Category	Common red flag indicators (non-exhaustive)
Client characteristics[140]	• Client is a PEP or one of his/her close relatives is a PEP (husband, wife, parents, etc.) • Client has close business, personal or family relationship with a public official connected to the client's business • Client has flawed background or reputation (e.g. convicted of a criminal offence; subject or linked to a judicial investigation; subject to negative press articles; corruption identified in previous audit reports) • Client is included on a list of sanctions (or is subject to another hit in KYC databases)
Client links to bribery and corruption	• Link between the client company and a negatively known company • Link between the client and a person who has been involved in a corruption case • Link between the client and a person who has been the subject of a judicial inquiry • Link between the client and a corruption case • Negative press about the client or his company and the allocation of public contracts • Incoming or outgoing flows from/to entities targeted in a corruption case
Documentation and source of wealth	• Client's wealth originates in a high-risk jurisdiction known for its high level of corruption • Client's wealth originates in high-risk business activities, known for frequent corruption • Origin of client's wealth not fully transparent, level of wealth not aligned with stated sources • Client tries to avoid or refuses to provide required documentation
Suspicious activities and transactions	• Client is introduced by intermediaries the bank does not regularly work with • Client uses proxies in its dealings with the bank • Client uses cash intensively • Client anticipates payments that cannot plausibly be commercially justified • Client requests unusual contract terms • Account activity shows high number of incoming or outgoing flows labelled "commission", "consultancy fees", etc. not explained by professional activity

[137] CRF, *Annual Activity Reports, Typologies*
[138] The Wolfsberg Group, *Wolfsberg Anti-bribery and Corruption (ABC) Compliance Programme Guidance*, 2017
[139] FATF, *Specific Risk Factors in Laundering the Proceeds of Corruption*, 2012
[140] Note, also applied to Beneficial Owners(s), Company Director(s), significant shareholder(s) or mandatories (if applicable).

Table 15: Red flag indicators for fraud risk in private banking (non-exhaustive)[141,142]

Category	Common red flag indicators (non-exhaustive)
Client characteristics	• Nature and/or purpose of the account or business relationship is unclear • Client uses recent corporate vehicles that are unnecessarily and unjustifiably complex (i.e. multi-tiered entities)
Client interaction and behaviour	• No face-to-face interaction with the client when opening the account • Client refuses any form of direct contact or communication • Client develops close private relationship with account manager • Conflict of interest is evident between client, relationship manager, external advisor and/or intermediary
Suspicious activities and transactions	• Client is introduced by intermediaries the bank does not regularly work with • Client uses proxies in its dealings with the bank • Client requests unusual contract terms • Account activity is not aligned with stated objectives or business

Table 16: Red flag indicators for circumvention of financial restrictive measures in private banking (non-exhaustive)

Category	Common red flag indicators (non-exhaustive)
Clients	• Legal persons • Frequent change of ownership • Change in ownership/control of a legal entity/legal arrangement shortly prior to a designation • Threshold technique: reduce of the ownership below 50%/25% by transferring the legal ownership to family member, close associates, business partners, nominees or third parties • Change/frequent change of the name of the client (legal persons) • Use of trust arrangements or complex corporate structures involving offshore companies or companies established in countries supporting sanctioned countries or multiple jurisdictions • Change in address for persons from countries subject to financial sanctions • Change of UBO from a person from a country subject to financial sanctions to an UBO with another nationality • Change of UBO to an UBO residing in countries known to support sanctioned countries • Customer reluctant to provide information (including on the transaction) • Use of enablers i.e. third party intermediaries such as advisory services to set up opaque ownership structures

[141] CSSF internal data, 2019
[142] CRF, *Annual Activity Report 2017,* 2018

	• Use of third parties to open bank account, operate legal entities/legal arrangements or pay on behalf of the designated person • Use of non-domestic banking relationships that may be in countries other than the country of incorporation of the company, or in offshore jurisdictions • Incorporation of new legal entities with poor quality or inexistent websites and by consequence a limited or inexistent online presence and no real economic purpose • Company located at the same address as designated natural and legal persons • Natural persons • Customer wealth/lifestyle/behaviour/transactions not consistent with the customer's profile • Reluctance to provide KYC/KYT information, avoiding personal contact, insisting on using an intermediary, avoiding communication after the formal entry into relationship • Use of out forged/altered documentation
Geographies	• IN/OUT flows of funds to countries where financial restrictive measures regimes are not considered • IN/OUT flows of funds to countries supporting sanctioned countries • Payments from complex structure/venture capital/private equity vehicle located in offshore jurisdictions that continue to support sanctioned countries or express neutrality in international forums such as the UN • Customers is physically located in an adjacent to countries concern
Transactions	• IN/OUT flows of funds to persons/beneficiaries through a financial institution established in a different company that the persons/beneficiaries • IN/OUT flows to family members/close associates of sanctioned persons • Unplanned flows OUT of funds shortly before or after the sanctions are taking effect • Change to instructions that appear contrary to history or business practices • Payments of unusual invoices at exorbitant or non-market rates from enablers • Domestic/European companies that have had long term business relationship with countries subject to financial restrictive measures • The customer provides incomplete information on the beneficiary when asked to provide additional information • The documentation of the transaction is vague and misleading • Use of real estate properties/transactions to hold wealth: particular attention shall be given to properties below/above their market value as well as the use of third parties with potential ties to sanctioned countries • Transactions split into smaller transactions in order to remain below a given threshold

- Sudden and unusual investments in high value assets
- Company used to trade with the sanctioned jurisdiction pre-designation and turnover of company increasing substantially since the designation
- Change of destination of exports after sanctions were adopted, but the type of goods and the payments remain the same as pre-sanctions
- Opening of bank accounts and transactions in neighbouring countries to sanctioned jurisdiction

Appendix B. Applicability for Investment Firms

Whilst this assessment focuses on private banks, many of the wealth management and ancillary services described are also provided by investment firms. Consequently, many of the findings of this report remain valid for investment firms.

Sub-sector overview

Investment firms are legal persons that require authorisation by CSSF. According to Article 4 (1) (1) of directive 2014/65/EU as amended, *'investment firm' means any legal person whose regular occupation or business is the provision of one or more investment services to third parties and/or the performance of one or more investment activities on a professional basis*.[143] According to Articles 24-1 to 24-9 of the LFS,[144] an investment firm may exercise different types of activities for which the authorisation criteria may vary. The precise services for which it is authorised must therefore be mentioned in its authorisation. The primary activity of investment firms typically is, however, portfolio management.

Investment firms constitute a smaller part of Luxembourg's financial services sector. As of the end of 2022, there were 95 investment firms established in Luxembourg, employing 1,958 staff.[145] Investment firms service approximate 157,000 clients (the vast majority of which are located outside of Luxembourg) and have AuM of approximately EUR 49 billion.'[146] These firms are supervised by the "Supervision of investment firms" department within CSSF.

Relevance of this risk assessment

Investment firms can provide a range of services to a geographically diverse group of clients. Most relevant for this assessment are portfolio management (Art 24-4 of the LFS) and, to some degree, investment advice (Art 24-5 of the LFS). Private portfolio managers in particular carry out asset management activities (including providing investment services and custody of financial instruments)[147] as well as some limited ancillary services (wealth structuring) that are also conducted by private banks.[148]

Where investment firms carry out the relevant activities described in this risk assessment, this assessment is applicable to them as well. In particularly, to further strengthen their understanding of ML/TF risks, relevant firms should consult the following sections:

- **Section 3: Luxembourg's private banking ecosystem**, to understand the key types of players in the market and how they interact;
- **Section 4: Inherent risk – threat assessment**, in particular the ML threat posed by tax crimes, corruption and bribery, and fraud;
- **Section 5: Inherent risk – vulnerability assessment**, as investment firms face the same vulnerabilities as private banks;
- **Section** Error! Reference source not found.**: Mitigating factors and residual risk assessment**, in particular the frequent off- and onsite findings;

[143] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments, as amended. See Article 1, point 9, of the LFS.
[144] Luxembourg, LFS
[145] CSSF, *Annual report 2022*, 2023
[146] CSSF internal data, 2023
[147] Note, Custody of cash is not authorised for investment firms. In accordance with Article 2(3) of the LFS, this activity is strictly reserved for banks.
[148] Due to the nature of the license held by investment firms, they cannot provide current account banking services, credit solutions, or insurance solutions.

- **Section 7**: **Emerging and increasing areas of risk**, in particular those related to outsourcing, new technologies and virtual assets.

Areas for further enhancement

All investment firms providing the products and services described in this assessment are required to take a proactive approach to mitigating ML/TF risks. They should use this risk assessment to continue improving their understanding of ML/TF threats and vulnerabilities, incorporate its findings into their own risk assessments, and further strengthen the mitigation measures they employ.

In line with AML/CFT Law, regulations and recently published circulars, CSSF has identified in this assessment a number of key recommendations for private banks. These apply equally to investment firms conducting the activities described in this document. CSSF will therefore monitor investment firms' adherence to this assessment's recommendations as part of its ongoing supervisory activities. **Firms should refer to Section 8** for further detail on CSSF's expectations, as well as some examples of how they may be able to show compliance with them.

Appendix C. Acronyms

Acronym	Definition	Acronym	Definition
ABBL	Luxembourg Banker's Association	IMF	International Monetary Fund
AEOI	OECD Automatic Exchange of Information	IR	Inherent risk
ACPR	Autorité de Contrôle Prudentiel et de Résolution	LFS	Law of 5 April 1993 on the financial sector in Luxembourg
AML	Anti-Money Laundering	LSI	Less significant credit institution
AuM	Asset under Management	ML/TF	Money Laundering and Terrorist Financing
BCL	Banque Centrale du Luxembourg	NGO	Non-Governmental Organization
BEPS	Base Erosion and Profit Shifting	OECD	Organization for Economic Cooperation and Development
BVI	British Virgin Islands	OSI	On-site inspection
CAA	Commissariat aux Assurances	PANC	Procédure Administrative Non-Contentieuse
CDD	Client Due Diligence	PB	Private Banking
CFT	Countering the Financing of Terrorism	PEP	Politically Exposed Person
CCO	Chief Compliance Officer	PSF	Professionals of the Financial sector
CRS	Common Reporting Standard	RBA	Risk Based Approach
CRF	Cellule de Renseignement financier	SAR	Suspicious Activity Report
CSSF	Commission de Surveillance du Secteur Financier	SI	Significant credit institution
ECB	European Central Bank	SME	Small and Medium Enterprises
EBA	European Banking Authority	SNRA	(EU's) Supra-National Risk Assessment
EC	European Commission	STR	Suspicious Transaction Report
EEA	European Economic Area	SSM	Single Supervisory Mechanism
ESMA	European Securities and Markets Authority	TCSP	Trust and Company Service Provider

EU	European Union	TF	Terrorist Financing
FACTA	US Foreign Account Tax Compliance Act	TFAR	Terrorist Financing Activity Report
FATF	Financial Action Task Force	TFTR	Terrorist Financing Transaction Reports
FTEs	Full Time Employees	TFVRA	Terrorism Financing Vertical Risk Assessment
HNW	High Net Worth	UHNW	Ultra-High Net Worth
ICMA	International Capital Market Association	US	United States of America

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu