Commission de Surveillance du Secteur Financier

ML/TF SUB-SECTOR RISK ASSESSMENT

PRIVATE BANKING

December 2019

Table of Contents

FOREWORD

Luxembourg is a dynamic and fast-growing economy and one of the leading financial centres in the world. At the heart of Europe with a highly-skilled and multinational workforce, our financial sector serves a diverse range of clientele both at home and abroad. Private banking is a substantial element of this, and increasingly Luxembourg is a true European hub for major institutions operating in this space. Banks licensed in Luxembourg provide private banking services throughout the European Union, and many have extended their offering to also service clients located further afield.

The growth of the financial sector has naturally increased Luxembourg's exposure to the evolving threat of money laundering and terrorism financing (ML/TF). Whilst the whole financial services sector is exposed, private banking activities are particularly at risk. This has been highlighted in the 2018 National Risk Assessment (NRA), confirming similar findings by the Financial Action Taskforce, the European Commission's Supra-National Risk Assessment and by supervisors in several other countries.

Luxembourg and CSSF are deeply committed to combatting ML/TF and ensuring that the risks arising from and within our jurisdiction are effectively managed and mitigated. In recent years, we have implemented a series of reforms to further strengthen our regime for combatting ML and TF (AML/CFT), and our efforts continue apace. The 2018 NRA has been critical to this process, strengthening the AML/CFT regime across both CSSF and supervised entities. This document is complementary to, and an extension of the National Risk Assessment. It is one of several dedicated sector and sub-sector risk assessments that CSSF is completing on areas highlighted as particularly high risk.

This inaugural Private Banking Sub-Sector Risk Assessment is a major step forward in the AML/CFT efforts of both CSSF and the private sector. The exercise has further strengthened our comprehensive and shared understanding of the inherent risks of private banking activities, the strengths of the current AML/CFT regime, and areas where mitigating measures could be developed further. It has been a joint and coordinated effort, led by CSSF and with input from stakeholders across the private banking industry and public sector.

Private banking was identified as an inherently high risk sector by the NRA. This document highlights several ML/TF threats and vulnerabilities that are particularly important for private banking in Luxembourg.

This risk assessment is a valuable tool for all stakeholders to better understand the ML/TF risks associated with private banking and the measures necessary to combat them. Supervised entities should use it to strengthen their understanding of ML/TF threats and vulnerabilities and further contribute towards the development of proportionate and effective controls. To this end, the assessment details observed best practices, common findings from supervision, and targeted recommendations the private sector should adopt. CSSF will monitor entities' adherence to these recommendations as part of our supervisory activities, and we have also committed to undertake several actions to strengthen our own approach.

I would like to thank all of those who have participated in this exercise for their valuable contributions, in particular the members of the ABBL-CSSF Private Banking Expert Working Group. I expect everyone

in the sector to continue strengthening their AML/CFT efforts so as to ensure that the AML/CFT framework remains effective and that Luxembourg remains a place where the private banking industry can thrive.

Claude Wampach

Director, CSSF

1. INTRODUCTION

The Financial Action Task Force (FATF) highlights private banking as a sector particularly exposed to money laundering (ML) and terrorism financing (TF). This view is echoed in the European Commission's (EC) Supra-National Risk Assessment (SNRA) and by supervisors in several countries.

In Luxembourg, private banking is a substantial part of the country's banking sector.[1] The sub-sector has been highlighted as having a "very high" inherent risk in the 2018 National Risk Assessment (NRA) and consequently CSSF has completed this sub-sector risk-assessment. The assessment identifies private banking activities which are particularly exposed to ML/TF and sets out areas where mitigating measures taken by CSSF and the private sector can be further strengthened.

CSSF has conducted this assessment from a supervisory perspective, albeit in close collaboration with the CSSF-ABBL Expert Working Group on ML/FT risks in private banking.

1.1. International ML/TF context for private banking

FATF has identified several areas of risk in private banking, including: "the culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs [and] high value transactions".[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 stated 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 EC's SNRA also highlights ML/TF risks related to private banking. According to the SNRA, "perpetrators are using private banking and wealth management for investing in shares for integration of criminal proceeds; title of shares to conceal beneficial ownership (BO) … [and] investment to justify criminal proceeds as profit". Accordingly, the EC rates the ML threat related to private banking as "moderately significant/significant".[5]

Supervisors in several other countries have also increased their scrutiny on the ML/TF risks associated with private banking. The UK Financial Conduct Authority (FCA) has highlighted the high inherent ML/TF risks in private banking, primarily due to the international client base and the difficulty to differentiate legitimate from suspicious activity in international financial centres.[6] Similarly, the French *Autorité de Contrôle Prudentiel et de Résolution* (ACPR) has issued detailed guidelines on specific AML/CFT measures related to private banking.[7]

[1] Luxembourg National Risk Assessment, 2018
[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 private banking services
[4] FATF, Specific Risk Factors in Laundering the Proceeds of Corruption, June 2012
[5] European Commission, Report from the commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Annex 1, 2017
[6] Financial Services Authority, *Review of private banks' anti-money laundering systems and controls*, 2007
[7] ACPR, *Lignes directrices relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme dans le domaine de la gestion de fortune*, 2014

1.2. Luxembourg ML/TF context for private banking

1.2.1. Luxembourg's 2018 NRA

In December 2018, Luxembourg published its NRA. The purpose of this was to identify, understand and assess the risks to which the country is exposed, and support the definition of the national AML/CFT strategy. Further details are provided below.

The NRA first identifies predicate offences (threats) that are particularly significant in Luxembourg. Starting from FATF's designated categories and using a weighted average of external and domestic exposure, the NRA concludes that drug trafficking, fraud and forgery, tax crimes and corruption and bribery are "very high" threats in Luxembourg. As shown below, these threats predominantly derive from international exposure. This is due to the international nature and cross-border exposure of the financial sector. In contrast, threat of ML from domestic crimes is significantly lower, due to Luxembourg's relatively low crime rate and limited presence of organised crime.

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

Designated predicate offence[8]	External exposure (75%)	Domestic exposure (25%)	Weighted av. exposure
Money laundering (average ML threat)	**Very high**	**Medium**	**Very high**
Drug trafficking	**Very high**	**High**	**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**
Participation in an organised criminal group and racketeering	**High**	**Medium**	**High**
Counterfeiting and piracy of products	**High**	**Medium**	**High**
Sexual exploitation, including sexual exploitation of children	**High**	**Medium**	**High**
Smuggling	**High**	**Low**	**High**
Robbery or theft	**Medium**	**High**	**High**
Trafficking in human beings and migrant smuggling	**Medium**	**Medium**	**Medium**
Insider trading and market manipulation	**Medium**	**Low**	**Medium**
Illicit trafficking in stolen and other goods	**Medium**	**Low**	**Medium**
Environmental crimes	**Medium**	**Low**	**Medium**
Illicit arms trafficking	**Medium**	**Low**	**Medium**
Counterfeiting currency	**Low**	**Low**	**Low**
Extortion	**Low**	**Very Low**	**Low**
Murder, grievous bodily injury	**Low**	**Very Low**	**Low**
Kidnapping, illegal restraint, and hostage taking	**Low**	**Very Low**	**Low**
Piracy	**Low**	**Very Low**	**Low**
Terrorism and terrorist financing	**Medium**	**Medium**	**Medium**

[8] Proliferation of weapons of mass destruction and its financing has also been added by FATF in its Recommendation 7 as another category of predicate offence (FATF, *Guidance on Counter-Proliferation Financing*, February 2018). However, this is considered out of scope for this report.

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

Table 2: Overview of Luxembourg's NRA – risks in the banking sector[9]

Sector	Inherent risk	Sub-sectors	Inherent risk
Banks	Very High	Retail & business banks	High
		Wholesale, corporate & investment banks	High
		Private banking	**Very High**
		Custodians and sub-custodians	High

Following the publication of the NRA, CSSF is now completing sub-sector risk assessments on several particularly high-risk areas. This assessment focuses specifically on private banking. It aims to identify activities which are particularly exposed to ML/TF, and further strengthen mitigating measures taken both by CSSF and the private sector. In doing so, it bridges the gap between risk assessments at sector-level (i.e. from the NRA) and entity-level. The document is therefore an extension of the NRA and complementary to CSSF Circular 18/702 detailing threats and current mitigation actions for private banking.

1.2.2. Private banking supervision in Luxembourg

CSSF is responsible for the supervision of the financial sector in Luxembourg. It supervises the professionals and products of the Luxembourg financial sector and is also in charge of supervising and enforcing compliance with professional obligations related to AML/CFT by these professionals. Within CSSF, the Banking supervision department performs market entry controls and exercises ongoing AML/CFT supervision of all banks in Luxembourg, including banks offering private banking services ("private banks").[10]

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.[11] CSSF communicates to the private sector on AML/CFT obligations and ML/TF risks on a regular basis. This includes through regulations, circulars, bilateral communication, participation to industry events such as conferences and direct interaction with representative industry bodies.

The Luxembourg Bankers Association (ABBL) has established in 2007 a dedicated private banking cluster to support the needs and development of players within the private banking in Luxembourg, via training, opinion building, working groups, position papers and other tools.[12] In 2019 CSSF and ABBL established a joint Expert Working Group for AML/CFT in private banking. This working group meets on a regular basis to discuss AML/CFT topics and strengthen the sub-sector's framework to combat ML and TF.

[9] 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).
[10] 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).
[11] FATF, *Guidance for a Risk-Based Approach: the Banking Sector*, 2014
[12] ABBL, *Private banking group webpage*

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.[13] Further details on the relevance of this assessment for these entities are provided in the Appendix.

[13] As defined in Article 24 of the 1993 Law of Financial Services.

2. STAKEHOLDERS, METHODOLOGY AND DATA

This section describes the stakeholders involved in the risk assessment and the methodology and data used. This methodology examines ML/TF threats and vulnerabilities (inherent risk) as well as mitigating factors and is closely aligned to that used in Luxembourg's NRA.

2.1. Stakeholders in this assessment

This report was written by **CSSF banking supervision department** in close collaboration with the following parties:

- **CSSF departments and experts:** internal AML/CFT teams and experts acted as key partners in drafting the assessment. The document was socialised within CSSF on a regular basis to discuss progress and solicit input and feedback, including from the investment firms' supervision department;
- **CSSF-ABBL Expert Working Group**: CSSF set up a working group in partnership with ABBL to exchange views on ML/TF vulnerabilities and mitigating factors. The working group includes selected bank executives and Chief Compliance Officers from private banks, as well as representatives from CSSF.

2.2. Methodology of the assessment

The assessment looks at ML/TF threats and vulnerabilities (inherent risk), and then at the measures put in place by both CSSF and the private sector to mitigate them. The methodology is based on CSSF's AML/CFT risk assessment policy and closely aligned to that used in Luxembourg's NRA.[14] The methodology is also aligned to the ESA's Joint Guidelines on Risk-Based Supervision and Joint Guidelines on ML/TF Risk Factors, to the EBA's Risk Factors Guidelines, to the FATF's Guidance for a Risk-Based Approach (Securities Sector) and to peer practices.

Inherent risk – Threats assessment

Threats are types of predicate offences generating illicit proceeds which could give rise to ML/TF. The objective of the 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 report examines the most relevant ML threats for private banking, considering "very high" and "high" threats highlighted in the NRA, as well as additional threats commonly associated with private banking.[15] The NRA threats are based on the FATF list of designated categories of predicate offence.[16]

TF threats are presented separately. The report highlights the low prevalence of TF via private banking and provides reasons behind this observation.

Inherent risk – vulnerability assessment

Vulnerability is the relative attractiveness of a sector or sub-sector for ML/TF purposes. The FATF defines vulnerabilities as "those things that can be exploited by the threat or that may support or facilitate

[14] 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).
[15] Luxembourg National Risk Assessment, 2018
[16] FATF Glossary

its activities".[17] This may also include the features of a particular sector, a financial product or type of service that make them particularly exposed to ML/TF risks.

Vulnerability arises from activities which are particularly exposed to abuse or misuse for ML/TF purposes. The objective is to determine the level of ML/TF risks posed by different private banking activities.

Vulnerability is driven by multiple factors, including the type and geographic exposure of clients, the use of intermediaries, the market size and structure, the activities and products offered and the use of external advisors.

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 ML/TF risks.

Mitigating measures are intended to cover the full lifecycle of supervision along the following dimensions: understanding of ML/TF risks, market entry (including both licensing and registration), rules setting and oversight, rules enforcement and detection.

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 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. This includes international sources (e.g. from international organisations, foreign competent authorities, industry bodies, academia), other domestic competent authorities (e.g. CRF, Parquet), CSSF internal data collected as part of supervisory measures, CSSF expert input, information provided by the private sector (e.g. via questionnaires, interviews or workshops) and other domestic sources. Where information was missing, the assessed level of risk has been increased, in line with a conservative approach recommended by FATF.

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

3. OVERVIEW OF PRIVATE BANKING IN LUXEMBOURG

Private banking is a substantial component of Luxembourg's banking sector.[18] The industry is specialised in cross-border services, with more than three quarters of private banking assets managed (AuM) in Luxembourg coming from foreign clients.[19] In recent years, the number of private banking clients has decreased, whilst total AuM has grown: this reflects an increasing focus on high-net worth (HNW) and UHNW (ultra-high-net worth) clients and a decrease of affluent client accounts.[20] Luxembourg's private banking sub-sector is quite fragmented, with the largest five private banks holding a significant market share, and many smaller institutions.[21] Most private banks in Luxembourg are foreign-owned and operate in Luxembourg as part of international groups.[22]

For the purpose of this assessment, the actors of the private banking ecosystem have been split into four categories:

1) **Private banks** provide personal and tailor-made products and services 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).

2) **Beneficiaries** 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 benefit from private banking activities.

3) **Intermediaries** facilitate interactions between private banks and beneficiaries and often maintain a regular relationship with the private bank or the client. For example, the actors in this category could be: Power of Attorney (POA) holders carrying out instruction 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.

4) **External advisors** are third-party specialist service providers that support beneficiaries and/or private banks with specialised services provided at specific occasions. For example, they can provide financial or legal expertise, trust or company services or assist private banks with specific aspects of client due diligence.

Note, some actors of the private banking ecosystem may assume different roles at different occasions or fulfil several of the above roles at the same time. For example, a licensed third party asset manager may also act as a business introducer and a POA holder may also provide TCSP services.

[18] As reported in Luxembourg National Risk Assessment (2018), additional areas of specialisation of the banking sector include insurance, the functions of custodian bank for investment funds and fund administration, and fund distribution.
[19] ABBL/CSSF, *Annual Private banking surveys*, 2013-2018. Based on geographic origin of private banking client's accounts
[20] CSSF, Internal data as of 31 December 2017
[21] CSSF, Internal data as of 31 December 2017
[22] CSSF, Internal data as of 31 December 2017

3.1. Private banks

Private banks provide diverse, personalized 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.[23]

Asset management activities are at the core of private banks' business model. Such activities can be split in two broad sub-categories:

- **Custody of financial assets** involves booking and safekeeping of cash, stocks, bonds or investment fund shares along with all related back office services, such as transaction execution (e.g. brokerage services) and settlement, dividend and interest collection and distribution, corporate action processing, tax reporting, etc.; and

- **Investment services** involves optimizing 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.[24,25]

Ancillary services comprise other services that can be split in four sub-categories:

- **Current account banking** comprises services to satisfy clients' basic banking needs, such as current accounts, payment services, credit cards or electronic banking;

- **Credit solutions** typically include credit lines to improve portfolio returns (e.g. margin lending) as well as loans unrelated to portfolio investments, including for real estate investments (i.e. mortgages and property finance);

- **Wealth structuring** involves advising on High New Worth (HNW) or Ultra-High Net Worth (UHNW) clients' global investment strategy and on the most appropriate legal or corporate structure to fit the client's needs for asset protection, succession planning or tax planning. It also includes creating bespoke personalised investment schemes. Wealth structuring is also offered by external advisors; and

- **Insurance solutions** comprises the distribution of life and non-life insurance products (e.g. property, automobiles, art, etc.) structured by insurance professionals. In Luxembourg, insurance professionals are supervised by the *Commissariat Aux Assurances* (CAA).

3.2. Beneficiaries

Beneficiaries can be either direct clients (i.e. account holders) or ultimate beneficiaries.

Private banking clients are typically classified based on the **assets that private banks manage on their behalf** (AuM). In the ABBL-CSSF annual survey, they are categorised in three groups: Affluent, High Net Worth (HNW) and Ultra-High Net Worth (UHNW) clients. Affluent clients hold AuM up to €1 MM; they still represent the majority of private banking clients in number (as of end of 2016) but hold a minority of the total value of AuM in Luxembourg. HNW individuals hold between €1 MM and €20 MM of AuM and represent about a third of total AuM in Luxembourg. UHNW individuals are the wealthiest

[23] Please note that this is an illustrative categorisation defined for the purpose of this risk assessment. This exercise considers private banks as all the banks that have declared private banking as their main or regular activity in the CSSF annual ML/TF risk assessment questionnaire.
[24] 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, which typically cannot ask for specific investment decisions (e.g. buying stocks from a specific company).
[25] 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).

clients, holding more than €20 MM in assets. As of 2017, while they represent a minority of the clients in numbers, they hold about half of total AuM in Luxembourg.[26]

The **geographic origin of AuM** of private banking clients in Luxembourg is diverse. According to the ABBL-CSSF annual survey and CSSF internal data, less than a quarter of private banking AuM comes from Luxembourg, while the rest of the assets come from abroad.[27] Among foreign private banking assets, about half of them come from countries within the EU, with a significant percentage from neighbouring France, Germany and Belgium. 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, the central European location including membership of the Eurozone, the diverse and high-quality services, and the concentration of experts and international workforce.[28]

Private banking clients can be **natural persons, legal entities or legal arrangements**.

Private banking beneficiaries may also be categorised according to additional criteria to understand the level of ML/TF risk. For example, they can be analysed according to their fiscal residency, nationality, source of wealth, net assets, beneficial owner activities (e.g. beneficiaries can be entrepreneurs or executives, or their wealth can be related to an inheritance and other sources).[29]

3.3. 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 introducing intermediaries, POA holders, and third-party managers.[30]

Introducing intermediaries are natural persons or legal entities serving private banks to grow their client base.[31] 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. 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 or cross-border asset management services provided to clients. While these group companies may also provide inputs for CDD on those clients, the private bank 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, accountants, 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.

[26] ABBL/CSSF, *Annual Private banking surveys*, 2013-2018
[27] Based on the classification from 2017 ABBL/CSSF survey, which considers the geographic origin / registration of clients' accounts and on CSSF internal data as of 31 December 2017.
[28] Association of the Luxembourg Fund Industry (ALFI), *Luxembourg: The Global Fund Centre*, November 2017
[29] Other categories exist such as the net assets of beneficiaries, the complexity of the group structure, the activities related to the beneficial owner, etc.
[30] 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.
[31] Also referred as "business finders" or third-party introducers, as defined in The Wolfsberg group, *The Wolfsberg AML Principles Frequently Asked Questions with Regard to Intermediaries,* 2012

Third-party managers act on behalf of clients as professional asset managers.[32] Third-party managers can represent one or more clients. They provide diverse investment services to clients such as discretionary asset management or advisory. They may be located in Luxembourg or abroad. In most countries, including Luxembourg, asset management services can only be provided by licensed professionals.

3.4. External advisors

External advisors are third-party specialist service providers that support beneficiaries and/or private banks with specialised services provided at specific occasions.[33] For example, these include: financial advisory services, legal advisory services, trust or company services, and client due diligence services.[34]

Financial advisory services: external professionals with specialist financial expertise may provide specific or tailored services to private banks and/or beneficiaries. 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.

Legal advisory services: legal professionals may provide services to implement the client's wealth structuring and investment services activities.[35] Lawyers and notaries are the main professionals involved in setting up legal arrangements, investment vehicles or any other relevant legal schemes to implement the client's tax and estate strategy or optimize investment services.

Trust or company services: beneficiaries or private banks themselves may also request support from trust or company service providers to optimise relevant investments or wealth structuring strategies. According to the 2004 AML/CFT Law and in line with FATF definition, there are five types of trust or company services:[36,37]

- Incorporation services consists in 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;
- 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;
- 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

[32] Also referred as "Managing intermediaries", as defined in the Wolfsberg group, *The Wolfsberg AML Principles Frequently Asked Questions with Regard to Intermediaries,* 2012
[33] 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.
[34] 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.
[35] 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
[36] Luxembourg, *2004 AML/CFT Law Chapter 1, Article 1, Paragraph 8(a) to 8(e)*
[37] FATF, *Methodology for assessing technical compliance with the FATF recommendation and the effectiveness of AML/CFT systems*, 2019

- Nominee shareholder services consist in acting as, or arranging for another person to act as, a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in accordance with European Union law or subject to equivalent international standards.

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 specialized professionals of the financial sector (among which family offices).

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 or UHNW customers. Private banks may request external expertise or group capabilities on specific CDD inputs (e.g. reports, access to specialised database, etc.) or may leverage clients' documentation in possession of group/sister companies to fulfil specific 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.

4. INHERENT RISK – THREAT ASSESSMENT

This purpose of this section is to understand and to assess the exposure of private banking activities to ML/FT threats[38] and determine those ML/FT threats that are most relevant for private banking in Luxembourg. The section is divided into three sub-sections:

1) **ML threats for private banking activities in all countries:** describes how private banking activities are most likely to be misused and/or abused in the layering and integration stages of ML (rather than the placement stage). This is due to multiple factors, such as the high value of transactions; the international nature of the business; and the complexity of some products and services;
2) **ML threats most relevant to private banking in Luxembourg:** identifies and assesses the three most critical ML threats to private banks in Luxembourg. These are tax crimes (primarily those committed by foreign individuals), corruption and bribery (primarily related to foreign corruption and bribery); and fraud;[39] and
3) **TF threats to private banking in Luxembourg:** identifies and assesses the nature of the TF threat to private banks in Luxembourg. This threat is low compared to retail banks and recent significant abuses/misuses are not known.

Note, the analysis that follows considers only inherent risk (i.e. risk before mitigating factors).

[38] "Risk can be seen as a function of three factors: threat, vulnerability and consequence" (FATF Guidance, *National Money Laundering and Terrorist Financing Risk Assessment*)
[39] Fraud here refers to two categories of predicate offence as defined in Luxembourg's NRA: 'Fraud and Forgery' and 'Insider Trading and Market Manipulation'.

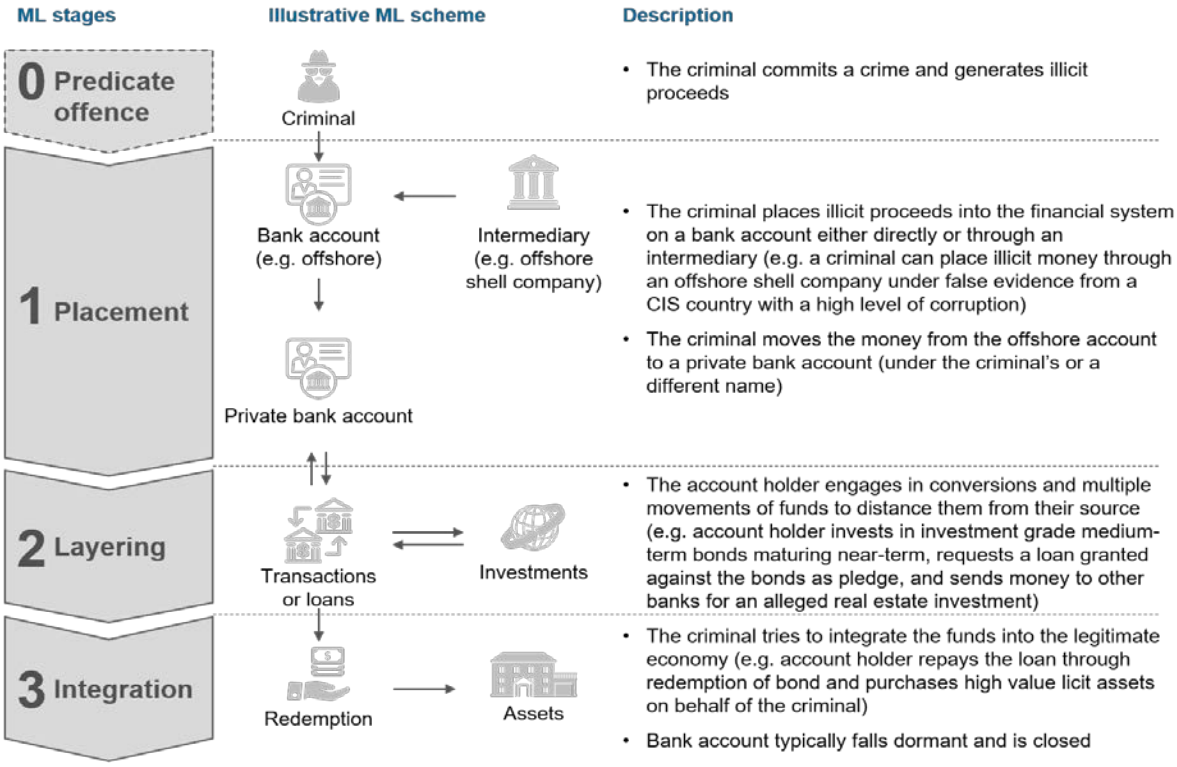
4.1. ML threats affecting private banking activities in all countries

Private banks are exposed to ML at all stages: placement, layering and integration.[40] 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.[41]

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.[42] Private banks can be abused or misused as the point of entrance of their clients' cash proceeds 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 transferred electronically from one investment or account to another and potentially across several geographies. Eventually, funds are returned to the criminal from what seem to be legitimate sources.[43]

Figure 1: Illustration of ML scheme through private banking



The exposure of private banks to layering and integration is due to multiple factors:

[40] FATF, *FAQ: How is money laundered?*
[41] Europol, *Financial Intelligence Group, Why is cash still king?,* 2015
[42] Europol, *Financial Intelligence Group, Why is cash still king?,* 2015
[43] Europol, *Financial Intelligence Group, Why is cash still king?,* 2015

- **High value of transactions:** Large investment volumes make it easier to introduce large sums of illicit proceeds, while high minimum investment requirements are less likely to trigger alerts. The alignment of objectives between portfolio manager and money launderer (i.e. wealth preservation) makes simulation of legitimate investor behaviour easier;
- **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 and offshore financial centres. This can be exacerbated by the use of foreign intermediaries;
- **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 and tax planning), can increase the opaqueness of the sub-sector and increase the difficulty in detecting ML;
- **Difficulty in identifying beneficial owners:** Although the majority of private banking accounts are held by private individuals, a significant share of private banking clients are legal entities or legal arrangements, for which the identification of beneficial owners can be more complex than for natural persons.[44] Complex legal structures might be used by criminals to hide their identity and position as beneficial owners;
- **The high wealth and investment sizes of clients:** Private banking clients are by nature wealthy and invest larger amounts of funds; and
- **Frequency of high value transactions:** Large value transactions are likely to occur more frequently in private banking than in other banking sectors, making the potentially illicit nature of large transfers more difficult to detect.

4.2. ML threats most relevant for private banking in Luxembourg

In Luxembourg, supervisory experience, suspicious activity and transaction reporting, as well as engagement with the Expert Working Group indicates that there are three predicate offences particularly relevant for the private banking sub-sector: (1) tax crimes; (2) corruption and bribery; and (3) fraud. Whilst Luxembourg is typically not the country of origin of these predicate offences or the placement funds resulting from them, private banks may be misused/abused for ML at the layering and integration stages.[45]

The following sub-sections therefore define these threats and assess the specific exposure of the private banking sub-sector in Luxembourg. Occasionally, information from global sources that is also relevant for Luxembourg may be used to complement more limited, Luxembourg-specific data.

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 EU SNRA as particularly

[44] Note, a register of beneficial owners was set up by the law dated January 13th 2019 with effect from March 1st 2019 implementing provisions of the fourth Anti-Money Laundering Directive into Luxembourg law (Loi instituant un Registre des bénéficiaires effectifs).
[45] Luxembourg National Risk Assessment, 2018. Note, it is at these two stages that CRF most commonly receive STRs or other information from Luxembourg-based institutions.

relevant for private banking.[46] Tax evasion (*escroquerie fiscale*) and aggravated tax fraud (*fraude fiscale aggravée*) are predicate offences in Luxembourg.[47,48]

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.[49] 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.[50] In contrast, misuse/abuse related to *domestic* tax evasion/fraud is likely 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 FDP vs. 1-1.1% in Germany, France and Belgium).[51] The relative exposure to tax crimes from foreign and domestic individuals is also reflected in the nature of cases investigated by CRF, as shown in the case studies below.[52]

Figure 2: CRF case studies of suspicious activity in banking related to possible tax crimes[53]

Provision of third-party accounts

"A Belgian national, residing for tax purposes in Thailand, holds an account with a Luxembourg bank, from which he regularly transfers funds to his daughter's bank account. These funds would come from a donation as well as the sale of land and buildings for a total amount of 2.1million EUR. Between 2015 and 2017, the account is debited of a total of 1million EUR to a law firm specialising in civil and property law in Spain for the acquisition of three apartments. In 2016, the person concerned stays in Belgium for 6 months. Then he returns to Thailand and regularly travels to Spain, the United States and Belgium. As a result of all these elements, the bank is unable to establish his tax compliance and terminates the business relationship."

Doubts on economic reasons for a loan

"A company whose tax residence is in Lichtenstein has a bank account with a Luxembourg bank. This company is requesting a loan of USD 10,000,000 which should be transferred to the private account of the economic beneficiary, resident for tax purposes in Ecuador, guaranteed by the latter's private funds which would be the result of his professional activity. According to open sources, the economic beneficiary is reportedly the president of an Ecuadorian company linked to corruption cases in Ecuador and his wife there would be politically exposed. However, in Liechtenstein, the granting of a loan by a company to its beneficiary would be considered as a distribution of hidden profits."

Transfer of the tax residence to a country that does not practice information exchange

[46] European Commission, *Report from the commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Annex 1*, 2017
[47] Law of 23 December 2016 and Circular CSSF 17/650, 2017
[48] 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).
[49] 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.
[50] See Section 5 for further details on inherent risk related to 'Clients and Geographies'
[51] 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)
[52] Note, these case studies related to the banking sector in general (i.e. not specifically to private banking).
[53] CRF, *Annual activity report 2017*, 2018 (Note, the text included here is a translation from the original French document)

"An individual of French nationality and French tax resident holds several accounts with a Luxembourg bank. Her husband, a French resident, has a power of attorney over these banking accounts. The holder declares that she is moving to China while her husband remains a French resident. There was a doubt that residence in China might be fictitious in order to hide possible assets from the French tax authorities."

In total CRF identified 1,440 suspicious transactions related to tax crimes in 2017 across all sectors. The majority of these (~50%) related to bank transfers, and a significant minority (~18%) to cash collection and payments).[54]

Luxembourg has put in place a strong legal and regulatory framework to combat international tax evasion. For example, legislation was introduced to implement the Organisation for Economic Co-operation and Development (OECD) Common Reporting Standard (CRS) for the automatic exchange of financial information. Luxembourg was rated "Largely Compliant" by the OECD as it had demonstrated progress on the deficiencies identified in the first round of reviews. These included improving access to information, developing broader Exchange of Information ("EOI") agreement networks, and monitoring the handling of increasing incoming EOI requests.[55] Luxembourg is also actively involved in the OECD Base Erosion and Profit Shifting (BEPS) initiative and has enacted legislation to address BEPS Action 13, on country-by-country reporting. Adding the aforementioned offences of tax evasion *(escroquerie fiscale)* and aggravated tax fraud (*fraude fiscale aggravée)* to the list of predicate offences for ML has also helped reduce the likelihood of such crimes by extending AML/CFT measures to these offences (e.g. KYC and Suspicious Activity Reporting (SAR) obligations).[56]

4.2.2. Corruption and bribery

Corruption and bribery includes the relevant offences defined across several parts of Luxembourg's Criminal Code, specifically: domestic bribery (private to public) as defined in Articles 240 et seq.; domestic bribery (private to private) as defined in Articles 310 et seq.; and corruption of foreign public officials as defined in Article 252.[57] These crimes have a significant impact on the development and health of economies worldwide,[58] undermining the rule of law and the principle of fair competition and often contributing to political instability and human rights abuses.[59] Globally, corruption and bribery are estimated to account for 2% of total proceeds of crime[60] and in recent years private banks have been implicated in several cases.

In Luxembourg, the primary exposure of private banks relates to *foreign* corruption and bribery. This is due to the international nature of the sub-sector's activity, the concentration of wealthy and politically exposed clients, and the use of third-parties and intermediaries. The nature of this exposure is reflected in suspicious reporting to CRF. Indeed, "almost all reports [received in 2017 and relating to corruption] concerned suspects with their residence abroad or having committed primary offences of corruption or illegal taking of interest abroad".[61] The nature of such exposure is described further in the case study

[54] CRF, *Annual activity report 2017*, 2018
[55] OECD Global Forum on Transparency and Exchange of Information for Tax Purposes, *Peer review report* released on March 18, 2019
[56] CSSF, *Circular CSSF 17/650*, 2017. While aggravated tax evasion was added as a new offence, tax fraud was already criminalised prior to 2017. With the 2017 tax reform the legislation has been strengthened and both offences are now also a predicate offence to ML.
[57] Luxembourg, *Code pénal*, 2018 (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)
[58] UNODC, *Annual report*, 2017
[59] Transparency International, *Why corruption matters*, 2019
[60] UNODC, *Annual report*, 2017
[61] CRF, *Annual activity report 2017*, 2018 (Note, refers to all sectors, not solely private banking)

below, concerning CSSF's thematic work in relation to the ML implications of alleged illicit activity involving the Estonian branch of Danske Bank A/S.

Figure 3: CSSF thematic review: Suspicious transactions involving the Estonian branch of Danske Bank A/S [62]

Context

Following the publication of media reports about significant volumes of suspicious transactions involving the Estonian Branch of Danske Bank A/S (Danske Estonia), CSSF contacted a number of banks to obtain more information on (1) potential transactions with Danske Estonia; (2) banks' conclusions from their own investigation of their monitoring of these clients and transactions; and (3) any actions taken or proposed to be taken as a result of their investigation.

The main purpose of CSSF's intervention was to ascertain whether banks had respected their professional obligations and monitored their clients and transactions adequately. Banks were also requested to review the effectiveness of their processes and procedures to ensure they were adequate to detect similar risks going forward.

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

Findings and Conclusions

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

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

In contrast, the threat from corruption of *domestic* origin is deemed to be relatively low in Luxembourg.[63] Transparency International ranks the country 8th out of 180 in its Corruption Perception Index, and the World Bank ranks Luxembourg 8th out of 247 in its Controls of Corruption Index.[64,65]

4.2.3. Fraud

Fraud in this section refers to a broad set of deceptive practices and incorporates two categories of predicate offence from Luxembourg's NRA, namely: 'Fraud and Forgery', 'Insider Trading and Market Manipulation'.

Globally, private banks can be abused or misused to launder the proceeds of various different types of fraudulent activity. These can range from simplistic frauds such as falsification, to more complex schemes. A non-exhaustive list of examples is outlined below:

[62] CSSF thematic work, 2019
[63] Luxembourg National Risk Assessment, 2018
[64] Transparency International, *Corruption Perception Index*, 2017
[65] World Bank, *Data Bank: Worldwide Governance Indicators, Control of Corruption*, 2016

- **Ponzi schemes**: investment schemes in which money from new investors is used to provide a return/repayment to previous investors;
- **Insider Trading**:[66] an individual or group trade on the stock exchange to their own advantage through having access to confidential information;
- **Advance fee fraud**: an investor seeks to reverse a previous investment mistake. A criminal offers a high price for worthless stock in exchange for a fee that must be paid in advance. When the fee is paid, the criminal disappears; and
- **Offshore scams**: a fraudulent advisor invites individuals to invest in a foreign country and does not send the money invested back, while law enforcement is often very complex for local authorities.

In addition to the above, CSSF has noted an increased number of fraud attempts over the internet by entities pretending to be licensed financial intermediaries or using the names of licensed financial intermediaries. These schemes often involve criminals trying to attract customers through an interesting offer of investment services by reference to Luxembourg's reputation as an international financial centre.

For private banks in Luxembourg, several factors indicate that fraud may be a material ML threat. These include the international exposure and geographically diverse client base of private banks, as well as the complexity and opacity of some products (e.g. wealth structuring activities). The use of third parties and intermediaries in private banking creates an additional element of risk, as illustrated by the case study provided below.

Figure 4: Fraud attempt in private bank through an external advisory[67]

Typology: Investment scam to convince private banking clients to invest in illicit schemes

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

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

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

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

When combined, all of 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.

[66] Note, 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'.
[67] CSSF Case Study, 2019

4.3. TF threats in private banking in Luxembourg

Terrorist financing refers to the financing of terrorism, terrorist acts, and of terrorists and terrorist organisations. It encompasses the raising, movement and use of funds by terrorist actors and is considered as one of the most important threats to global security.[68]

The most relevant form of TF is movement of funds and the most exposed activities are those related to products and services offered by retail banks.[69] In particular, terrorist actors could misuse/abuse banking products to move funds *cross-border*, 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 attacked is planned). The low value nature of such activity makes such activity difficult to detect, with research showing that 75% of violent extremism cases in Europe between 1994 and 2013 cost less than $10,000.[70]

Figure 5: Example of terrorist financing through private banking [71]

Case study: Terrorist financing through private banking

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

As regards Luxembourg, the NRA notes that the banking sector as a whole is exposed to TF. The CRF received 234 terrorist financing activity reports (TFARs) and terrorist financing transaction reports (TFTRs) in 2017, and 68 in 2016.[72,73] Whilst this increase (+240%) is likely to be related to improved reporting, it could also be correlated with an increase in TF activity in Luxembourg.

For private banks specifically, exposure to TF is driven by their size, international nature, and aforementioned ability to facilitate rapid cross-border financial flows. However, they are typically less exposed to TF than retail banks on account of the closer relationship between the client and the bank (e.g. use of relationship managers). Accordingly, recent significant abuses or misuses are not known and the CRF received only one TFAR and one TFTR from private banks in 2017.[74]

[68] FATF, *International standards on combating money laundering and the financing of terrorism and proliferation – the FATF recommendations*, 2012
[69] FATF, *Emerging Terrorist Financing Risks*, 2015
[70] Forsvarets Forskningsinstitutt, Oftedal, Emilie, *The financing of jihadi terrorist cells in Europe*, 2015
[71] FATF, Financing of Recruitment for Terrorist Purposes, January 2018
[72] CRF, *Annual Report 2017*, 2019
[73] CRF, *Annual report 2016*, 2017
[74] CRF, *Annual Report 2017*, 2019

5. INHERENT RISK – VULNERABILITY ASSESSMENT

The vulnerability assessment evaluates the relative exposure of the two core activity categories and four ancillary activity categories identified in Section 3.1 to ML risks. Overall the activities of the sub-sector are considered **inherently High risk**.[75] A summary of the results is provided below.

Table 3: 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 six identified activity categories. CSSF's analysis shows that the first two risk factors affect ML/TF inherent risk equally across all private banking activities (Section 5.1), while the impact of market structure, activities and products, and external advisors may vary from one activity category to the next (Section 5.2).

5.1. Risk factors impacting all areas of private banking activities in Luxembourg

Two risk factors have been identified as affecting ML/TF inherent risks across all private banking activities: clients and geography, and intermediaries.

Clients and geography: The large number of clients (143,000 according to the ABBL-CSSF annual survey)[76] and the prevalence of big and potentially more sophisticated accounts may increase the complexity of private banking activities performed in Luxembourg. Clients with AuM larger than €1 MM hold a large and increasing majority of private banking AuM in Luxembourg; these can be split in clients with AuM larger than €20 MM (holding about half of the total AuM) and clients with AuM between €1

[75] 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.
[76] ABBL/CSSF, *2018 Annual Private banking survey*, data as of end of 2017

MM and €20 MM (holding about a third of the total). While clients with AuM smaller than €1 MM represent most private banking clients in number, they hold a minority of total AuM in Luxembourg.[77]

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/FT risk (e.g. as concerns tax crimes or corruption) for the bank. A non-negligible (albeit decreasing) share of private banking clients in Luxembourg are legal persons, and the use of more complex structures (e.g. to offer increased flexibility and privacy to clients) may decrease transparency regarding beneficial ownership. For instance, insurance wrappers may be exposed to ML/TF risks (e.g. through tax crimes, market abuse) as private banks may not have full visibility on the client's beneficial ownership (in the case of insurance wrappers, the account is held by an insurance company which has the client relationship).

In terms of geographical origin, according to the CSSF-ABBL survey and CSSF internal data, the majority of AuM come from Europe, but outside Luxembourg. This may complicate the identification of beneficial owners and the origin of their wealth. Less than a quarter of private banking AuM comes from Luxembourg account-holders, while the remaining three quarters come from account-holders located abroad.[78,79] While the diverse, international clientele reflects the attractiveness of Luxembourg as an international private banking centre, the cross-border origin of most AuM may decrease the level of transparency on the funds invested in the sub-sector.

According to private banks' own internal risk assessments, a large percentage of their clients have high ML/TF risk. The percentage of high-risk clients in Luxembourg private banks is much higher than in other banking sub-sectors such as retail banks.[80] Clients from more remote jurisdictions with known AML/CFT deficiencies may contribute proportionally more to the sub-sector's ML/FT risk than their share of AUM or account numbers might indicate.

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

Introducing intermediaries work on behalf of private banks to grow their client base. Private banks that are subsidiaries or branches of foreign-owned banks may rely on their parent and/or sister companies to grow their client base through referrals or cross-border asset management services provided to clients. Several private banks in Luxembourg (whether part of larger groups or standalone banks) have reported making use of external introducing intermediaries (e.g. lawyers, financial advisors, accountants, fund managers or other financial institutions)[81], which may be a non-negligible source of business for them. Introducing intermediaries may be from any jurisdiction and are typically not required to be registered or supervised in Luxembourg. As a result, the services they offer may decrease the level of transparency between private banks and their clients (and beneficial owners), especially when private banks rely on intermediaries to provide inputs to conduct client due diligence (CDD), such as by collecting client documentation.

The presence of POA-holders with signatory authority over a client's account and acting on behalf of the client may also decrease transparency by limiting the direct contact between the client and the bank, making it more difficult to "know the client" or understand his/her transactional account behaviour. As

[77] ABBL/CSSF, *2017 Annual Private banking survey*, data as of end of 2016
[78] ABBL/CSSF, *Annual Private banking surveys*, 2013-2018
[79] Note that as the geographic origin of assets is assessed through the origin of client accounts, it is likely the foreign-based beneficial owners represent an even larger share than 76% of AuM.
[80] CSSF internal data, 2017
[81] CSSF internal data, 2017

with introducing intermediaries, POA-holders may be from any jurisdiction and are not required to be registered or supervised in Luxembourg, which may further increase complexity.

Finally, third-party managers act on behalf of their clients and may be the only direct point of contact of private bankers. The presence of third-party managers limits face-to-face interactions between private banks and their clients and may limit the understanding of the client's global investment strategy, portfolio of investments, history of business activities and transactions. On the other hand, where third-party managers are authorised and supervised, they may however provide an additional level of ML/TF control (as they will have their own AML/CFT obligations in respect to their clients).

5.2. Other inherent risk factors across private banking activities

The impact assessment of the remaining three risk factors (market structure, activities and products, and external advisors) may vary across the six identified areas of private banking activity. These are therefore reviewed activity by activity in the following paragraphs.

5.2.1. Custody of financial assets

Custody of financial assets includes booking and safekeeping of cash, stocks, bonds and investment fund shares along with all related back office services.

Market structure: According to the CSSF-ABBL survey, the private banking sub-sector in Luxembourg generates about €1.7 BN of revenues and accounts for €363 BN assets under management.[82] Within this sub-sector, custody of financial assets is the main activity.

Private banks in Luxembourg have a wide variety of business models. Most private banks considered for this risk assessment are part of international groups. There are several large banks, but also many smaller institutions competing for a share of the market.[83] Due to their limited scale of activities, smaller or stand-alone private banks may in some cases have less sophisticated AML/CFT controls in place and, where they are not part of a group, will not be able to rely on the group's expertise, policies, processes, and international network. Smaller banks may also specialise in specific types of clients (e.g. affluent vs. UHNW clients only, or clients from specific geographies or affiliated with a specific group). This focus, together with their limited size and resources, may impact on the risk level of smaller private banks.

Activities and products: Custody services and products have a relatively 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 sometimes arise due to the significant volume of the activity (as described above), the remote nature of the services (provided without direct client contact or to clients in foreign countries, from Luxembourg) or limitations in monitoring capabilities.[84]

External advisors: Whilst standard custody services are not particularly exposed to ML/TF risks, the involvement of international specialist advisors can increase the level of risk, in particular when both the client and its advisor are located in remote jurisdictions. External advisors typically decrease the direct interaction between private banks and their clients and may increase even further the distance between the private bank and the ultimate beneficial owner. They can also reduce the bank's visibility

[82] ABBL/CSSF, *2018 annual Private banking survey*, data as of end of 2017
[83] CSSF internal data, 2017
[84] European Commission, Report from the commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Annex 1, 2017

on the client's investment goals and objectives, limiting the possibility to detect unusual investments and transactions.

5.2.2. Investment services

Investment services include services for optimizing clients' investment mix in line with the defined investment strategy. There are two main kinds of investment services: discretionary asset management services and investment advisory.[85,86]

Market structure: Investment services are less relevant in terms of volume than custody of financial assets; however, they remain an important activity in Luxembourg. Clients with AuM larger than €1 MM hold the vast majority of assets under management in Luxembourg; these categories of clients typically require more complex advisory and investment solutions in response to specific and often sophisticated investment needs (e.g. access to specific funds and/or markets). On the contrary, clients with AuM smaller than €1 MM may favour less complex advisory and investment solutions and invest in more generalist funds, limiting their downside exposure (e.g. funds with risk diversification requirements such as UCITS).

Activities and products: Investment advisory services include the provision of advice related to relatively standardised investment products available from the bank or schemes that are somewhat tailored to the needs of the client. It is typically difficult to conceal illicit activities through such standardised products.

Discretionary asset management services have a moderate ML/TF exposure, because investments are typically in products that are relatively transparent (e.g. mutual funds, hedge funds) and because investment decisions are typically taken by the private bank. The bank's investment decisions follow a pre-defined and agreed investment strategy, for which clients cannot give direct buying orders (e.g. they cannot request to allocate part of their discretionary management portfolio to buy shares in a specific company at a certain point in time). Concealing illicit activities is therefore difficult.

Whilst the opportunity for misuse or abuse or investment services in private banking is relatively limited, there remains some level of risk. For example, Figure 6 below presents a hypothetical case in which a private banking client uses non-publicly available information for making an investment decision. The client then layers illicit proceeds through simple investment orders.[87]

Figure 6: Typology: Insider information to generate illicit proceeds and launder money[88]

Insider trading refers to the buying or selling of a security based on material non-public information about the security, in violation of a fiduciary duty or other relationship of trust and confidence.[89]

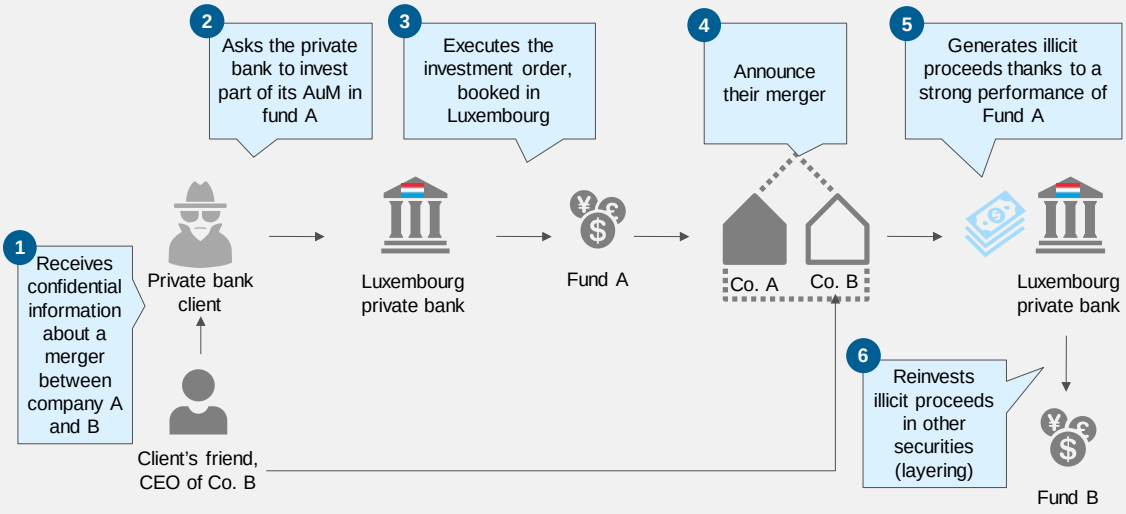
The following example illustrates how clients may use insider information to generate proceeds and launder money through investment services of private banks. The following steps may occur:

1. A private banking client meets with an old friend who is now the CEO of Company B, a competitor of Company A. Over the discussion, the CEO discloses non-public information

[85] 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, which typically cannot ask for specific investment decisions (e.g. buying stocks from a specific company).
[86] 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, etc.).
[87] Note, the use of "inside information" is not common in Luxembourg. Of the 5,740 predicate offences reported to CRF in 2017, only 28 involved "market abuse" (which includes insider trading). See: CRF, *Annual Report 2017*, 2019.
[88] Similar typologies may be found in the following report: FATF, *Money Laundering and terrorist financing through the securities sector*, 2009
[89] FATF, *ML/TF in the Securities sector*, 2009

about a future merger to be announced between Company A and B, which would make the new merged company a profitable market leader;

2. The client uses its knowledge to ask its private bank to invest in Fund A, which is the main shareholder of Company A;
3. The private bank invests part of the client's portfolio in Fund A, executing the client's request;
4. Company A and Company B announce their merger a few weeks later and the value of the merged company increases;
5. The client makes significant illicit proceeds thanks to the strong performance of Fund A when selling its shares in the fund. Illicit proceeds, generated thanks to insider information, go back to its Luxembourg private bank account; and
6. Then, the client reinvests illicit proceeds in other securities to distance funds from their origin (layering). The Luxembourg private bank executes the transaction.



External advisors: Investment services may involve external advisors, particularly when clients are looking for specific financial expertise (e.g. investment in niche sectors) or fiscal advantages (e.g. tax-efficient investment structure). External advisors are typically chosen for their financial, legal or fiscal expertise. The use of advisors may increase complexity of specific investment schemes, especially when it involves parties located in several jurisdictions and/or cross-border investment activity.

5.2.3. Current account banking

Current account banking includes services to satisfy clients' recurring banking needs. They may be all traditional banking services, such as deposit accounts, payment services, credit cards and standard savings solutions.

Market structure: All private banks typically offer current account banking services as ancillary services for all their clients. These services allow clients to address most of their deposits, liquidity and payment needs, as well as to transact on their own.

Current account banking services are typically standardised and do not vary depending on the business model of private banks. They are however a common type of services provided by private banks in Luxembourg and are therefore significant in volume. Additionally, smaller private banks may have less sophisticated AML/CFT controls in place (e.g. transaction monitoring systems) than their larger peers, making the detection of suspicious account movements initiated by the client (e.g. in relation to bribery and corruption) more difficult.

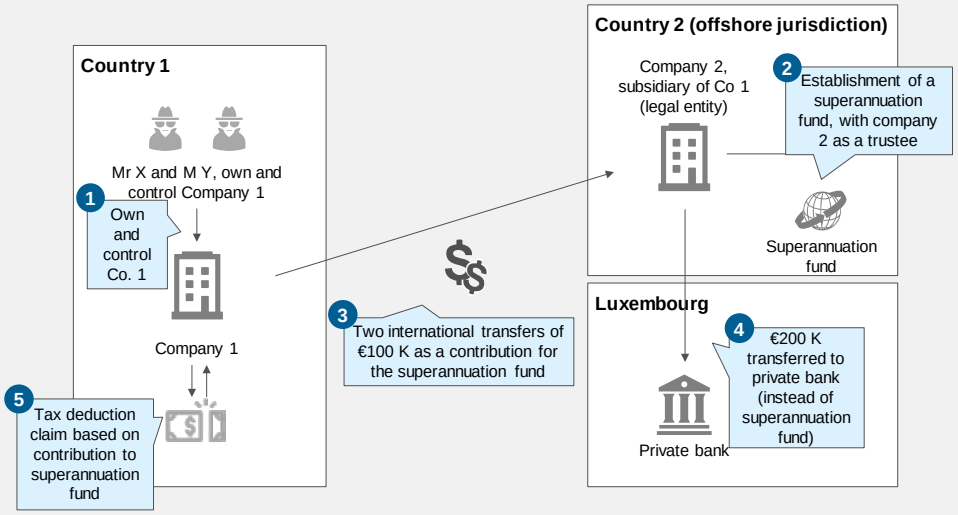
Activities and products: Management of current/savings accounts, cash deposits and withdrawals, electronic payments (e.g. through credit cards and clients transacting on their own account) are key current account banking activities and expose private banks to significant ML/TF risk. For example, cash withdrawals and deposits are a common method of ML/TF due to the anonymity provided by cash and the difficulty of monitoring for suspicious activity.[90]

Electronic payment services are also highly exposed to ML/TF. Whilst private banks are able to trace the direct recipient/sender of payments, the increasing volume of funds transferred electronically makes payments with funds from illicit proceeds increasingly difficult to detect.[91] The often cross-border nature of such payments further increases risk.

Figure 7: Typology: Tax avoidance through international transfers[92]

The following example outlines how international transfer services may be abused or misused to obtain illicit proceeds from tax deductions:

1. Two individuals X and Y own and control Company 1;
2. The two individuals instruct their accountant to establish a superannuation fund in an off-shore jurisdiction, for which Company 2 (established in the same off-shore jurisdiction and controlled by the same two individuals) acts as trustee of the fund;[93]
3. Company 1 transfers €100,000 for each of the two individuals to Company 2, as a contribution to the superannuation fund (for a total of €200,000);
4. Company 2 transfers the €200,000 to a newly established account in a private bank in Luxembourg, rather than to the superannuation fund. The two initial individuals X and Y control the account indirectly; and
5. Company 1 subsequently claims deductions in its own jurisdiction for the €200,000 offshore superannuation contribution in its tax return. The tax authorities assess company 1 as liable for less tax than it should have been, thereby avoiding its tax obligations.



External advisors: For current account banking, external parties are not typically used.

[90] 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
[91] FATF, *Money Laundering using New Payment Methods*, 2010
[92] Inspired by the Australian Transaction Reports and Analysis Center, *Typologies and Case studies report*, 2014
[93] A superannuation fund is a pension program created by a company for the benefits of its employees.

5.2.4. Credit solutions

Credit solutions cover credit lines to improve portfolio returns (e.g. margin lending) as well as loans unrelated to portfolio investments, including for real estate investments (i.e. mortgages and property finance).

Market structure: Private banks provide loans to their clients as a typical ancillary activity to core asset management. According to CSSF internal data, most private banks granted loans to their clients in 2017. Loans can also be a selling argument to attract new clients and thus an area for competition among banks.

Activities and products: ML/TF risks are typically higher for credit solutions unrelated to investment services activities (e.g. mortgages). Credit solutions could for example be obtained by pledging illicit assets as collateral.[94,95] The bank can seize the collateral and sell it if the client defaults on its loan payments. When credits unrelated to investment services are backed with collaterals from foreign or even offshore jurisdictions, it will become be more complex for private banks to assess the origin of funds at the basis of the pledged assets (as detailed in the typology below).

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. margin lending) are typically less exposed to the above ML/TF risks. Margin lending mostly answers short and medium-term treasury needs linked to a client's investment strategy. 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, without need for an additional collateral.

The typology below illustrates how credit solutions unrelated to investment service activities (in this case an international mortgage) could, hypothetically, be abused through use of collateral from illicit proceeds.

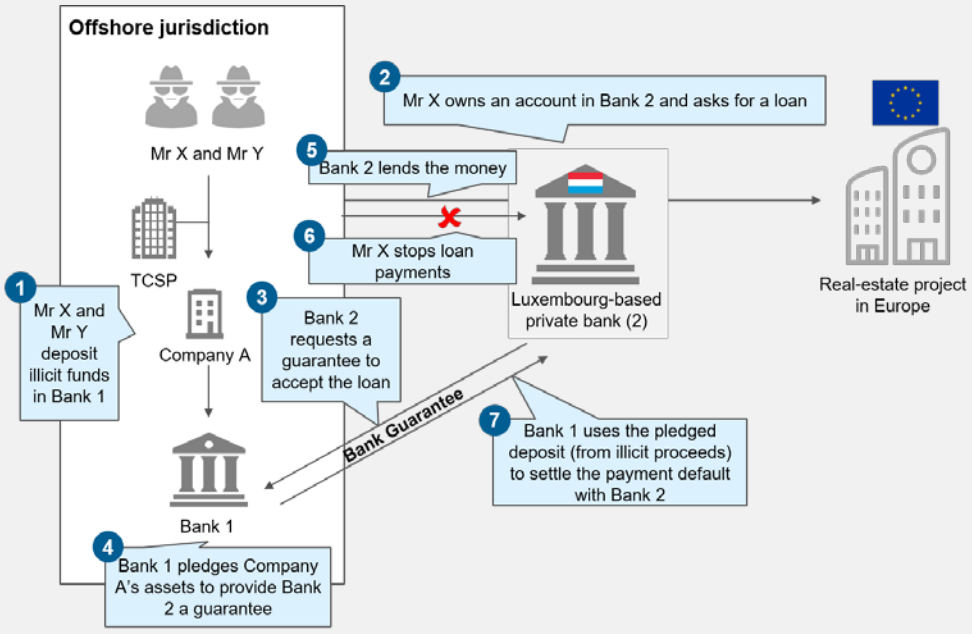
Figure 8: Typology: Use of collateral from illicit proceeds to finance real estate investments[96]

The following example illustrates how mortgages (and more in general other credit solutions) can be abused or misused by using collaterals generated from illicit activities. The following steps may occur:

1. Mr X and Mr Y deposit illicit funds via one of their corporate vehicles (Company A) into an account at Bank 1. Company A is in an offshore jurisdiction[97] 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. 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;
3. 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;

[94] 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 2004 AML/CFT Law, Article 3.2.c and CSSF Regulation 12-02, Article 24).
[95] 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).
[96] Similar typologies may be found in the following report: FATF, *Money Laundering and terrorist financing through the real estate sector*, 2007
[97] 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

4. Mr X arranges for Bank 1 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 accepts to provide the bank guarantee to Bank 2, based on company A's pledged deposit. The money deposited in Bank 1 originates from the illicit activities of Mr X and Mr Y. If Bank 2 were to withdraw the guarantee on Bank 1, Bank 1 would use the deposit pledged by Company A to settle the payment with Bank 2. 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;
5. Bank 2 lends the money to Mr X. Through the loan by Bank 2, Mr X can provide a valid reason for the money used to finance the real estate investment. Instead, the collateral originates from illicit activities;
6. Mr X initially makes loan and interest payments to Bank 2 using income from the licit real estate investment. After a few payments, Mr X stops paying the payment of the principal and the interest on the loan; and
7. Based on the loan agreement and the banking terms, Bank 2 calls on the bank guarantee from Bank 1. Bank 1 uses the pledged deposit to settle the payment to Bank. Mr X keeps the clean money from the loan. Hence, the pledged deposit is laundered.



External advisors: The use of external specialists to optimise wealth management may involve complex credit solutions that could make detection of ML/TF risks challenging. 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.

5.2.5. Wealth structuring

Wealth structuring includes 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 also includes creating bespoke personalised investment schemes. Wealth structuring is offered by some private banks, but more often by external advisors.

Market structure: In Luxembourg, the volume of wealth structuring services offered by private banks themselves is relatively limited since international and large clients (High-Net-Worth and Ultra-High-Net-Worth) typically use external financial advisors for their global wealth structuring services. Wealth structuring may also be performed by the parent or sister company of the Luxembourg private bank based in the country of residency of the client as a number of global private banks offer these services.

Activities and products: 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.

External advisors: Wealth structuring activities often involve specialist external advisors, mainly TCSPs and legal experts. Their involvement (and the complexity of their services) may reduce transparency and increase the distance between the private bank and the ultimate beneficial owner. TCSPs typically set up legal entities or legal arrangements fully tailored to the client and may provide additional services such as representation, domiciliation, fiduciary/trustee or nominee shareholder services for a client's structures. Legal experts may provide similar services: specialised lawyers may help optimize tax strategies, while notaries may help define optimal real estate schemes.

5.2.6. Insurance solutions

Insurance solutions involve the distribution of life and non-life insurance products structured by insurance professionals.

Market structure: Private banks are not the issuer of insurance. There is currently no "bank-insurer", possessing a licence both as a credit institution and an insurance company in Luxembourg. However, they may conclude or negotiate insurance products with their clients through insurance companies (with whom they have a partnership). They may also directly provide insurance brokerage services, provided they have been authorised to do so by the CAA (the supervisory authority in charge of supervision of the insurance sector in Luxembourg). Insurance companies are subjected to the same professional obligations under the 2004 AML/CFT Law as banks. The ML/TF exposure associated with market structure is therefore limited.

Activities and products: The distribution of non-life insurance solutions is less exposed to ML/TF, mainly because such products do not have an inherently high ML/TF risk. The non-life insurance sub-sector is considered as medium inherent risk in the NRA.[98] Insurance products are less flexible than most other financial services (e.g. loans, payment services): they often pay out against pre-defined event, have no surrender value, no investment elements and the premiums are generally of lower value.[99]

While some life insurance products are exposed to ML/TF, their distribution by private banks presents a limited exposure. Private banking clients may subscribe to some insurance products that are exposed to ML/TF, such as insurance wrappers or life insurance contracts that are transferable to other beneficial owners.[100,101] The most important risk factor is the lack of visibility on beneficial owners of the insurance products. Since private banks may conclude or negotiate these products with existing clients, the exposure to this risk is less relevant (e.g. insurance wrappers sold to a private banking client in Luxembourg). Moreover, 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, which ensures an additional layer of AML/CFT checks on clients.[102]

[98] Luxembourg National Risk Assessment, 2018
[99] FATF, *Guidance for a risk-based approach: Life Insurance Sector*, 2018
[100] Luxembourg National Risk Assessment, 2018
[101] "*Contrats d'épargne placement ou de capitalisation*", "*contrat de capitalisation au porteur*" are examples of bearer insurance contracts; insurance wrappers are life insurance policies invested in internal dedicated funds with a large quota of private equity.
[102] Luxembourg National Risk Assessment, 2018

External advisors: The distribution of insurance products may involve external advisors, which may increase complexity.

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:

1) **Risk mitigation by private banking professionals**: describes the mitigating measures put in place by the private sector. These can be grouped into four main areas, which follow professionals' AML/CFT obligations as described in the 2004 AML/CFT Law: ML/TF risk assessment; customer due diligence; cooperation with competent authorities; and internal organisation, governance and training;

2) **Risk mitigation by CSSF:** describes the mitigating measures put in place by CSSF. These can also be broadly categorised into four areas: promotion of understanding of ML/TF risks (e.g. via regular communication with the private sector); market entry controls; oversight and supervisory activities (e.g. onsite inspections); and enforcement of compliance with AML/CFT obligations (e.g. administrative fines); and

3) **Most frequent off- and on-site findings**: highlights common findings from supervisory activity. Typical weaknesses including insufficient documentation; not reporting ML/TF suspicions to the FIU; and a lack of critical analysis with respect to the plausibility of some transactions.

As discussed further below, whilst some areas for improvement have been identified in private sector controls, overall significant mitigating actions are in place. This means that although the activities of the sub-sector are considered **inherently high risk** (see previous section), the **residual risk** (i.e. risk after mitigating measures are applied) is **medium-high**.[103,104]

Table 4: Summary of ML/TF residual risk – vulnerability assessment

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

[103] Note, 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.
[104] 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).

6.1. Risk mitigation by private banking professionals

Private banking professionals apply a range of methods to mitigate ML/TF inherent risks. Following professionals' AML/CFT obligations as described in the 2004 AML/CFT Law, these have been grouped hereafter in four main areas: (1) ML/TF risk assessment; (2) customer due diligence; (3) internal organisation, governance and training; and (4) cooperation with competent authorities. The nature of these mitigating factors is outlined at a high-level below.[105]

6.1.1. ML/TF risk assessment

Private banks generally take appropriate steps to **identify, assess and understand their ML/TF risks** (for customers, countries or geographic areas; and products, services, transactions or delivery channels). In most cases, risk assessments are documented, kept up-to-date, and relevant risk factors are considered before determining the level of overall risk and the appropriate level and type of mitigation required. The ML/TF risks of new products and business practices (including new distribution mechanisms and the use of new or developing technologies for both new and pre-existing products) is also typically assessed. Risk assessment information is also provided to competent authorities when requested.

6.1.2. Customer due diligence

Private banks apply a number of measures in relation to customer due diligence (CDD). These include the CDD process at onboarding (which typically involves an "acceptance committee") and ongoing due diligence throughout the business relationship.

Customer due diligence[106]

When customers are onboarded, private banks assess the ML/TF risk and complete a **due diligence process (CDD)**, applying a risk-based approach. This involves identifying the customer and verifying his identity using reliable, independent source documents and data. It also involves identifying the beneficial owner and obtaining 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 high-risk lists (e.g. using open-source databases such as WorldCheck). Where ML/TF risks are higher, an **enhanced due diligence (EDD)** may be performed. This is required for business relationships and transactions with natural and legal persons from higher risk countries and is typically also used for clients such as PEPs. In certain circumstances (e.g. in relation to PEPs), senior management approval is required before establishing such business relationships.

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 committee ("**the acceptance committee**") provides the authorisation. These committees are composed of individuals from different departments within the organization (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 2004 AML/CFT Law.[107] Whilst such third-party professionals

[105] Note, the description of mitigating factors reflects observed practice and is not intended to be exhaustive.
[106] Note, this is sometimes referred to as completing "Know Your Customer" (KYC) checks.
[107] The 2004 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

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 having recourse to an external service provider for CDD services must draw up a contract setting out the service provider's detailed obligations, while the responsibility entirely remains with the bank.

Ongoing due diligence

In addition to CDD/EDD at onboarding, private banks typically 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 keep all necessary records on transactions (both domestic and international), as well as records obtained through CDD measures, account files and business correspondence, and the results of 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, a dedicated private banker takes care of each private banking client (i.e. each client has a dedicated relationship manager). As outlined in the ESA's Risk Factor Guidelines, "the relationship manager's close contact with the customer will facilitate the collection of information that allows a fuller picture of the purpose and nature of the customer's business to be formed (e.g. an understanding of the client's source of wealth, why complex or unusual arrangements may nonetheless be genuine and legitimate, or why extra security may be appropriate)".[108] This can serve to strengthen 1st line controls. Note, however, that this may also "introduce conflicts of interest if the relationship manager becomes too close to the customer",[109] meaning 2nd line oversight is important.

6.1.3. Cooperation with competent authorities

Private banks cooperate with competent authorities through several different channels. These include monitoring transactions and activities 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 CSSF-ABBL Expert Working Group.

Transaction monitoring and suspicious activity reporting

On an ongoing basis, private banks typically **scrutinize the transactions undertaken by clients** to ensure those conducted are consistent with the banks' knowledge of the customer, their business and risk profile, and source of funds. These activities include 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. These activities also extend to ensuring that private banks' AML/CFT obligations in respect to wire transfers are met (e.g. all cross-border wire transfers of €1,000 or more are accompanied with required information).

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 the CRF. Private banks currently **report suspicious activity (SARs) and suspicious transactions (STRs) to the CRF**, including for attempted transactions. The CRF has reported that the quality of ML/TF detection is continuing to improve, and this has been facilitated by (among other things) improved cross-border exchange of

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.
[108] ESA, *The risk factor guidelines*, 2018
[109] ESA, *The risk factor guidelines*, 2018

information.[110] The Common Reporting Standard has had a significant impact in this respect (see below).

Figure 1: CRS and automatic exchange of information[111]

The Common Reporting Standard (CRS) is a normalized and automated solution to exchange information on bank accounts between tax authorities. The CRS intends to equip tax jurisdictions with an effective tool to fight against offshore tax evasion by enhancing exchange of information on resident's assets held abroad. The Standard for Automatic Exchange of Financial Information in Tax matters (the "standard") seeks to maximise effectiveness and minimise costs for all stakeholders.[112]

Following a G20 request to improve international cooperation to fight against tax crimes, the Organization for Economic Cooperation and Development (OECD) Council approved the creation of a Common Reporting Standard (CRS) in July 2014.

The two main components of the Standard are the CRS and the Multilateral Competent Authority Agreement (MCAA). The CRS details the due diligence rules for financial institutions to follow to collect and report information required for automatic exchanges. The MCAA specifies the financial information to be exchanged and provides a link from the CRS to the legal basis for exchanging such information. The MCAA avoids the need for several bilateral agreements. An implementation handbook, clarifications on the CRS and the MCAA and some guidance on technical solutions provide additional information to facilitate the implementation of the Standard, while ensuring data safeguards, confidentiality, transmission and encryption.[113] The CRS is increasingly used, as 86 jurisdictions have exchanged information bilaterally under the standard in 2018.[114]

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 or conferences. Through the ABBL, private banks have also established an Expert Working Group with CSSF on AML/CFT, which has played an important role in the drafting of this assessment. In addition, in respect to specific ML/TF investigations, private banks provide, upon request, any additional information requested by the CRF or other relevant authorities (e.g. law enforcement).

6.1.4. Internal organization, governance and training

Private banks have put in place **policies, controls and procedures** to effectively mitigate and manage ML and TF risks. These typically include defining ML/TF risk appetite and ML/TF key risk indicators that are approved by the Board of Directors, communicated to employees, and monitored on a regular basis. They also include documenting key policies and procedures (e.g. in relation to CDD; client risk assessment; transaction monitoring; wire transfers; correspondent banking; new technologies; reliance on third parties; foreign branches and subsidiaries; reporting of suspicious transactions; and tipping off) and ensuring employees adhere to the ABBL's code of conduct (which sets out ethical expectations for all employees). 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

[110] CRF, *Activity report,* 2017. "Le but affiché est d'atteindre un bon niveau d'efficacité du dispositif de lutte contre le blanchiment et le financement du terrorisme"
[111] OECD, *Standard for Automatic Exchange of Financial Information in Tax matters – Implementation handbook*, 2018
[112] OECD, *Standard for Automatic Exchange of Financial Information in Tax matters – Implementation handbook*, 2018
[113] OECD, website
[114] OECD, *Global Forum on Tax Transparency marks a dramatic shift in the fight against tax evasion with the widespread commencement of the automatic exchange of financial information*, November 2018

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

According to the CSSF circular letter dated December 3, 2012, all banks and investment firms have to stick to the **"comply or explain" principle** regarding their adhesion to the ICMA Private Wealth Management Charter of Quality. Hence, all banks and investment firms are requested to inform CSSF whether they have signed the Charter or whether there are reasons leading not to sign it.

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 development in ML/TF and preventative measures, and periodically distribute AML/CFT-related documentation is a best practice.[115]

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.

6.2. Risk mitigation by CSSF

The mitigating factors employed by CSSF are grouped into four main factors, each of which is described below: (1) Understanding of ML/TF risks; (2) Market entry; (3) Oversight and supervision; and (4) Rules enforcement.

6.2.1. Understanding of ML/TF risk

CSSF and private banks understand ML/TF risks and communicate regularly on these issues (e.g. on a bilateral basis and through workshops or conferences). CSSF and the ABBL private banking cluster have established an Expert Working Group on AML/CFT, and CSSF uses a range of mechanisms to provide guidance to the sub-sector on AML/CFT obligations and ML/TF risks (e.g. circulars). Further guidance is provided by several international organisations.[116] The relative maturity of the sector should also be taken into consideration when evaluating understanding of ML/TF risks.

6.2.2. Market entry

CSSF's market entry controls prevent 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.[117] The market entry process is based on a dual assessment performed by the ECB and CSSF, except for

[115] 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.
[116] For example, the International Capital Market Association (ICMA) published a Private Wealth Management Charter of Quality in 2012, which CSSF required all private banks to adopt.
[117] FATF, *Recommendations - Immediate Outcome 3*, 2019

branches of third country banks. As part of the Single Supervisory Mechanism (SSM) framework, the ECB is the Competent Authority to license all new significant and less significant credit institutions within the Eurozone. The Ministry of Finance is the Competent Authority to license all branches of third country banks in the country. Nevertheless, CSSF is the entry point for all bank licensing and qualifying holding applications in Luxembourg and CSSF's assessment of these applications includes an analysis of ML/FT risk based on the business model and business plan presented by the Applicant.

6.2.3. Oversight and supervision

CSSF's oversight and supervision of private banks spans both offsite and onsite activities. CSSF AML/CFT offsite banking supervision division performs ongoing offsite supervision on all banks (e.g. through ongoing desk-based review, regular interactions with supervised entities and an annual AML/CFT questionnaire). An on-site inspection division is dedicated to performing full scope, targeted or thematic AML/CFT on-site inspections, the frequency and intrusiveness of which have increased in recent years. Additionally, Luxembourg has recently established a beneficial ownership register, improving transparency over those with significant and/or control interesting in private banking products/accounts.[118,119] Such a register will provide professionals with a direct view of the beneficial owner(s) of Luxembourg-registered entities and accounts.

6.2.4. Rules enforcement

In recent years, CSSF imposed administrative sanctions on several banks for non-compliance with AML/CFT obligations. CSSF's sanctioning powers were further strengthened and broadened in 2018, enhancing CSSF's ability to ensure compliance with AML/CFT obligations. Over 2017 and 2018, CSSF imposed €19 MM in administrative fines for AML/CFT breaches to banks, five of which are private banks.[120]

[118] The register of beneficial owners was set up by the law dated January 13th 2019 with effect from March 1st 2019 implementing provisions of the fourth Anti-Money Laundering Directive into Luxembourg law (Loi instituant un Registre des bénéficiaires effectifs).
[119] The Law transposes Article 30 of the 4th Anti-Money Laundering Directive, by creating a register of beneficial owners of corporate entities. The registered entities may include, for example, public/private limited companies, partnership, non-profit organisations, together with Luxembourg-based branches of foreign companies and mutual funds ("fonds communs de placement").
[120] Based on public information

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 5: 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 • Providing control functions, especially compliance, with **sufficient means and necessary management support** • Installing **effective and appropriate technology** to monitor & detect suspicious transactions • Ensuring **close oversight over branches and subsidiaries** • Ensuring **clear allocation of responsibilities** between 1st and 2nd lines of defence • 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
Most common findings	• **Incomplete documentation**/information on the origin of wealth, the identity of legal persons and beneficial owners as well as powers of attorney • Insufficient diligence to understand the **ownership and control structure** of the client • **ML/TF classification** of the account only based on the risk criteria linked to account holder • ML/TF risks linked to **clients and country risk** not appropriately assessed • **Insufficient supporting documentation** for incoming/outgoing transactions • **Lack of critical analysis** with respect to the plausibility of some transactions • **Insufficient involvement of Compliance** function • ML/TF **suspicion not reported** (or reported late) **to the FIU**

7. AREAS FOR FURTHER ENHANCEMENT

Recommendations specifically targeted towards private banks will contribute to increasing their understanding of ML/TF risks and AML/CFT obligations (Section 7.1). Moreover, this exercise has also allowed to identify initiatives to enhance CSSF's current regulatory and supervisory framework (Section 7.2).

7.1. 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 2004 AML/CFT Law, regulations and recently published circulars, including CSSF circular 18/702, CSSF has identified a number of key recommendations to private banks. 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 6: 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 BoD in a written, detailed document, including the types of clients, geographies, products and services the bank wishes to cover (or avoid) and the resources and tools required to properly control the risk
2	**Engage the Board of Directors in the bank's AML/CFT strategy, policies and processes**	Board minutes demonstrating engagement with AML/CFT issues
3	**Reflect the findings from this report in the internal risk assessments**	Internal risk assessments that clearly reflects findings of this risk assessment
4	**Promote a strict compliance risk culture throughout the whole organization, in particular at the level of the first Line of Defence**	Appropriate training programmes in place across all three Lines of Defence, including 1st Line, and qualitative targets set for RMs
5	**Ensure robust processes are in place to reliably identify Beneficial Ownership and critically appraise the origins of funds/source of wealth**	Documented procedure for identifying beneficial ownership, in line with stated risk appetite and ability to evidence its effectiveness
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 FTE as well as technical resources & budgets allocated to AML/CFT activities justified based on 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 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**[121]	AML/CFT measures clearly documented at both Group and branch/subsidiary level, with evidence that the central AML/CFT functions effectively control the implementation and respect of group wide policies and procedures
9	**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**[122]	
10	**Collaborate closely with competent authorities to ensure Luxembourg has an effective national AML/CFT framework**	Provide prompt and accurate responses to requests by CSSF, the CRF or the Parquet; share best practices or provide feedback on publications (e.g. sharing information within and beyond the private banking AML/CFT EWG)
11	**Report promptly suspicious activities and transactions to the CRF**	STR reporting in line with risk exposure
12	**Implement effective technology solutions to strengthen the AML/CFT framework across key processes such as KYC, and transaction monitoring and reporting**	Evidence of use of newer technology solutions as part of key AML/CFT processes
13	**Adjust and enhance AML/CFT mitigating actions in light of emerging trends to sustain effectiveness of AML/CFT controls and adapt to structural changes in the market**	Ability to demonstrate control enhancements in response to changes in risk exposure

7.2. 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, summarized below.

CSSF will promote understanding of AML/CFT obligations and ML/TF risks. CSSF intends to actively support the efforts from the industry in improving their understanding of AML/CFT obligations and ML/TF risks. To achieve this, CSSF is undertaking several initiatives, including the formalisation of the AML/CFT Expert Working Group with the ABBL private banking cluster, the organisation of additional AML/CFT conferences with the private sector, the issuance of additional guidance, and the sharing of this risk assessment.

[121] FATF, Recommendation 18
[122] FATF, Recommendation 18

CSSF will continue to improve the effectiveness of supervision. CSSF is committed to enhancing the effectiveness of AML/CFT supervision within the private banking sector. For instance, using a broader set of remediation and enforcement measures.

CSSF will further enhance data availability to support offsite supervision. CSSF is committed to improving data availability and quality to perform offsite AML/CFT supervision. This covers both data obtained from the sector (e.g. by refining and enhancing the existing AML/CFT questionnaire) as well as data created by CSSF during its own supervisory activities (e.g. with latest technological solutions) or exchanged with other competent authorities

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 details on ML/TF red flag indicators can be found in publications including:

- CRF, Annual Activity Report 2017 (2018)
- FATF, Guidance for a risk-based approach, Securities Sector (2018);
- FATF, Guidance for a risk-based approach, Life Insurance Sector (2018);
- CSSF, Circular CSSF 17/650 (2017)
- The Wolfsberg Group, Wolfsberg Anti-bribery and Corruption (ABC) Compliance Programme Guidance (2017)
- FATF, ML through the physical transportation of cash (2015);
- FATF, ML and TF vulnerabilities of legal progressions (2013);
- FATF, Specific Risk Factors in Laundering the Proceeds of Corruption (2012)
- The Wolfsberg Group, AML guidance on credit/charge card issuing and merchant acquiring activities (2009); and
- FATF, ML and TF through the real estate sector (2007).

Table 7: Red flag indicators for fiscal offences in private banking (non-exhaustive)[123,124,125]

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* • 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*
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

[123] CSSF, *Circular CSSF 17/650*, 2017
[124] CRF, *Annual Activity Report 2017,* 2018
[125] For additional details see, for example, Honk Kong Monetary Authority, *Anti-Money Laundering Controls over Tax Evasion*, 2015.

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 is not interested in earning a 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 organization structure is not consistent with the documentation recoded 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 (2017)*

Table 8: Red flag indicators for corruption/bribery in private banking (non-exhaustive)[126,127,128]

Category	Common red flag indicators (non-exhaustive)
Client characteristics[129]	• 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's business is carried out in high risk jurisdictions • 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 convicted person • 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 • Link between the prospect and a customer who has been involved in a corruption case • Link between a company related to the client and the aware of public contracts • Link between funds from targeted entities and 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 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 requires payment of a commission before or immediately after winning a contract • Client anticipates payments that cannot plausibly be commercially justified • Client requests unusual contract terms • Notification of an entry order130

[126] CRF, *Annual Activity Report 2017,* 2018
[127] The *Wolfsberg Group, Wolfsberg Anti-bribery and Corruption (ABC) Compliance Programme Guidance*, 2017
[128] FATF, *Specific Risk Factors in Laundering the Proceeds of Corruption*, 2012
[129] Note, also applied to Beneficial Owners(s), Company Director(s) and other significant shareholder(s) (if applicable).
[130] An entry order is one that is used to enter a trade at a specified price level. If the trade never reaches that price level then the entry order is not executed.

Table 9: Red flag indicators for fraud in private banking (non-exhaustive)[131,132]

Category	Common red flag indicators (non-exhaustive)
Client characteristics	• Nature and/or purpose of the account or business relationship is unclear • Client uses corporate vehicles that are unnecessarily and unjustifiably complex (i.e. multi-tiered entities) • Conflict of interest is evident between client, relationship manager, external advisor and/or intermediary
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
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 requires payment of a commission before or immediately after winning a contract • Client requests unusual contract terms • Performance is not aligned with investment strategy

[131] CSSF internal data, 2019
[132] CRF, *Annual Activity Report 2017,* 2018

APPENDIX B. APPLICABILITY FOR INVESTMENT FIRMS

Whilst this assessment focuses on private banks, some of the wealth management and ancillary services described are also provided by investment firms. Further details on the relevance of this assessment for these entities is provided below.

Sub-sector overview

Investment firms are professionals of the financial sector as defined in Articles 24 to 24-11 of the Law of 5th April 1993.[133] Whilst these Articles encompass several different types of professional,[134] the primary activity of the sector is private portfolio management. As described in Article 24-3 of the 1993 Law, "private portfolio managers are professionals whose activity consists of managing portfolios in accordance with mandates given by clients on a discretionary client-by-client basis where such portfolios include one or more financial instruments".[135]

Investment firms constitute a smaller part of Luxembourg's financial services sector. As of the end of 2018, there were 97 investment firms established in Luxembourg, employing 2,115 people.[136] Investment firms service approximate 100,000 clients (the vast majority of which are located outside of Luxembourg) and have AuM of approximately €30 BN.[137,138] These firms are supervised by the *Entreprises d'investissement* (EI) supervisory department within CSSF.

Relevance of this risk assessment

As described above, investment firms provide a range of services to a geographically diverse group of clients. Most relevant for this assessment are those services provided by Private Portfolio Managers.[139] These professionals carry out asset management activities (including providing investment services and custody of financial instruments)[140] as well as some limited ancillary services (wealth structuring) that are also conducted by private banks.[141]

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

- **Section 3: Private banking overview**: to understand the key types of players in the market and how they interact;

[133] Luxembourg, *Law of 5th April 1993 on the financial sector, as amended*, 2019
[134] Included in the scope 'Investment Firms' are several different types of professional: investment advisers (Article 24 of the 1993 Law); brokers in financial instruments (Article 24-1 of the 1993 Law); commission agents (Article 24-2 of the 1993 Law); private portfolio managers (Article 24-3 of the 1993 Law); professionals acting on their own account (Article 24-4 of the 1993 Law); market makers (Article 24-5 of the 1993 Law); underwriters of financial instruments (Article 24-6 of the 1993 Law); distributors of units/shares in UCIs (Article 24-7 of the 1993 Law); financial intermediation firms (Article 24-8 of the 1993 Law); investment firms operating an MTF (Multilateral Trading Facility – a type of trading facility under MiFID II) in Luxembourg (Article 24-9 of the 1993 Law); and investment firms operating an OTF in Luxembourg (Organised Trading Facility – a type of trading facility under MiFID II) (Article 24-10 of the 1993 Law).
[135] Luxembourg, *Law of 5th April 1993 on the financial sector, as amended*, 2019
[136] CSSF, *Annual report 2018*, 2019
[137] CSSF, *Annual report 2018*, 2019
[138] CSSF internal data, 2019
[139] Note, Investment Advisors may also carry out some relevant activities, however the materiality of this is considered relatively low.
[140] Note, Custody of cash is not authorised for Investment Firms. In accordance with Article 2(3) of the Law of 5th April 1993 on the financial sector, this activity is strictly reserved for banks.
[141] Due to the nature of the license held by investment firms, they cannot provide current account banking services, credit solutions, or insurance solutions.

- **Section 4: Inherent risk – threats**: in particular, the ML threat posed by tax crimes, corruption and bribery, and fraud; and
- **Section 5: Inherent risk – vulnerabilities**: in particular, the vulnerabilities associated with custody of financial assets, investment services, and wealth management;
- **Section 6: Mitigating factors and residual risk**: in particular, the common observations from offsite and onsite inspections.

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, and further strengthen the mitigation measures they employ.

In line with 2004 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 7** 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	ICMA	International Capital Market Association
AEOI	OECD Automatic Exchange of Information	IMF	International Monetary Fund
ACPR	Autorité de Contrôle Prudentiel et de Résolution	IR	Inherent risk
ALCO	*Association Luxembourgeoise des Compliance Officers*	LFF	Luxembourg For Finance
ALRiM	Luxembourg Association for Risk Management	LSI	Less significant credit institution
AML	Anti-Money Laundering	MCAA	Multilateral Competent Authority Agreement
AuM	Asset under Management	MLRO	Money-Laundering Reporting Officer
BCL	Banque Centrale du Luxembourg	ML/TF	Money Laundering and Terrorist Financing
BEPS	Base Erosion and Profit Shifting	MM	Million
BN	Billion	NGO	Non-Governmental Organization
BVI	British Virgin Islands	OCCRP	Organized Crime and Corruption Reporting Project
CAA	Commissariat aux Assurances	OECD	Organization for Economic Cooperation and Development
CAGR	Compounded Annual Growth Rate	OSI	On-site inspection
CAC	Commissaire aux Comptes	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	RR	Residual risk
CSSF	Commission de Surveillance du Secteur Financier	SAR	Suspicious Activity Report
ECB	European Central Bank	SI	Significant credit institution
EBA	European Banking Authority	SME	Small and Medium Enterprises
EC	European Commission	SNRA	(EU's) Supra-National Risk Assessment
EEA	European Economic Area	STR	Suspicious Transaction Report

EI	Entreprises d'Investissement	**SSM**	Single Supervisory Mechanism
EIOPA	European Insurance and Occupational Pensions Authority	**TCSP**	Trust and Corporate Service Provider
ESMA	European Securities and Markets Authority	**TF**	Terrorist Financing
EU	European Union	**TFAR**	Terrorist Financing Activity Report
FACTA	US Foreign Account Tax Compliance Act	**TFTR**	Terrorist Financing Transaction Reports
FATF	Financial Action Task Force	**UHNW**	Ultra-High Net Worth
FCA	UK Financial Services Authority	**UNODC**	United Nation office on Drugs and Crime
FTEs	Full Time Employees	**US**	United States of America
GCC	Gulf Cooperation Council	**6AMLD**	6 Anti-Money Laundering Directive (European Union)
HNW	High net worth		

Commission de Surveillance du Secteur Financier

283, route d'Arlon

L-2991 LUXEMBOURG

Tel.: (+352) 26 251-1

Fax: (+352) 26 251-2601

E-mail: direction@cssf.lu

Website: http://www.cssf.lu