2023 AML/CFT Conference

Dedicated to Specialised Professionals of the Financial Sector (“PFS”)

30 January 2023

cssf
Commission de Surveillance du Secteur Financier

Agenda

- Risk self-assessment and RC report: purpose and content
- ML/TF Vertical risk assessment – Legal persons and legal arrangements
- Vertical risk assessment - Terrorist financing
- Insights from the FIU for Specialised PFS
- AML/CFT Expert working group for Specialised PFS
- Register of fiducies and trusts - obligations and requirements

Risk self-assessment and RC report:

Purpose and content

ML/TF Risk appetite:

Article 4 (4) of CSSF Regulation N° 12-02

- means the level of risk a professional is prepared to accept
- is a written statement clearly defining the framework of the entity's business and strategy (e.g. targeted clients, targeted transactions, services, etc.)
- is approved by the Board of Directors and implemented by the authorised management
- should be communicated to the whole staff in a precise, clear and comprehensible form
- policies, procedures and controls shall be consistent with the defined ML/TF risk appetite

cssf

Risk self-assessment:
Legal and regulatory basis

- Article 2-2 (1) of the amended AML/CFT Law dated 12 November 2004,
- Article 4 (1) of the amended CSSF Regulation N° 12-02
- CSSF Circular 11/529

Sources:

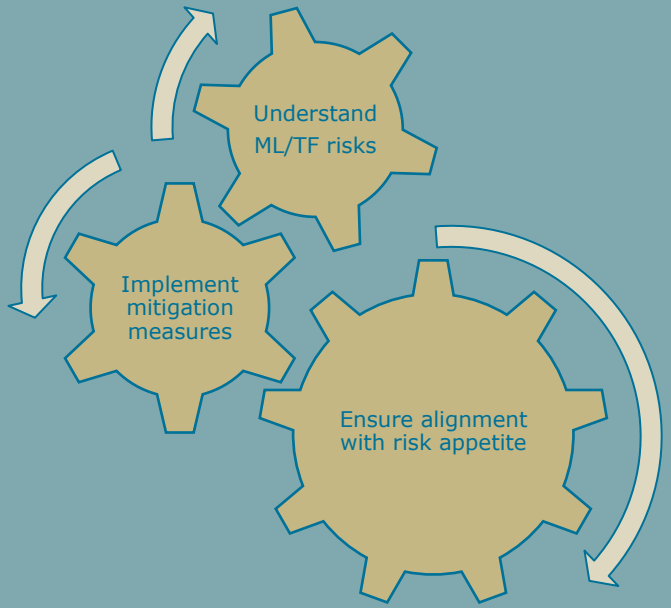
- Supranational risk assessment
- National risk assessment
- Vertical risk assessments
- Sub-sectorial risk assessments
- Joint guidelines issued by the three European Supervisory Authorities

Risk self-assessment: purpose

Helps the professional:

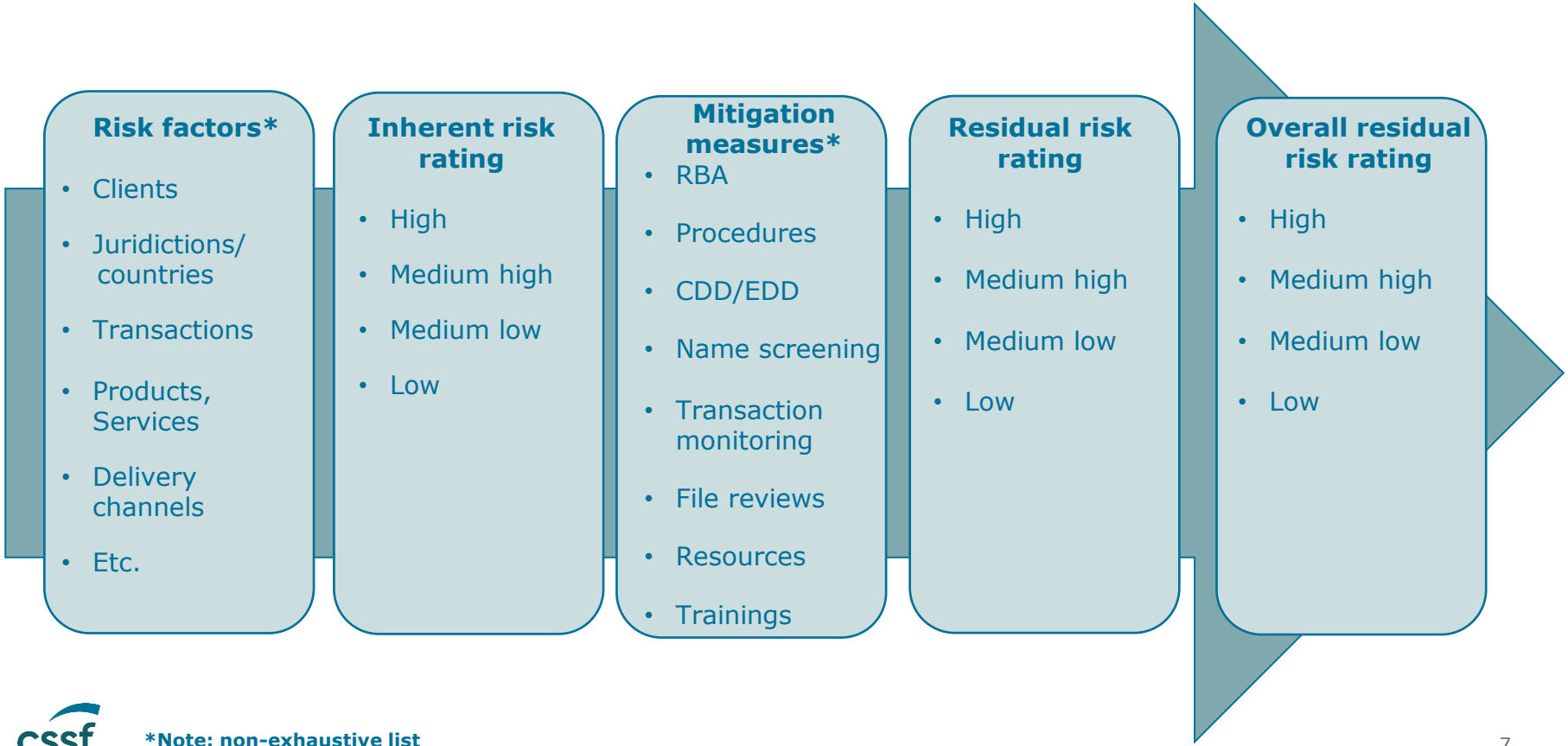
- to identify, assess and understand the ML/TF risks to which it is exposed
- to implement the right mitigation measures and apply a risk based approach
- to ensure that the overall residual risk falls within the scope of the risk appetite
- to complete the CSSF's annual AML/CFT questionnaire

Provides the CSSF with an insight of the ML/TF risks to which the entity is exposed and on its mitigation measures



Risk self-assessment: content

Article 2-2 (1) of AML/CFT Law, CSSF Circular 11/529



*Note: non-exhaustive list

Risk self-assessment

- Risk self-assessment should be reviewed on a regular basis and if needed, adjusted.

- In case of new products, business practices, use of new or developing technologies, the professional should **before** the launch or use :

  ⟹ review the risk appetite,

  ⟹ assess the ML/TF risks,

  ⟹ put mitigation measures in place.

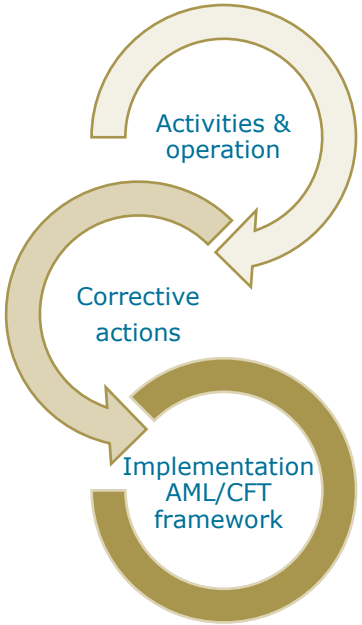
RC report:

Regulatory basis

Requirement to prepare a RC report is laid down in

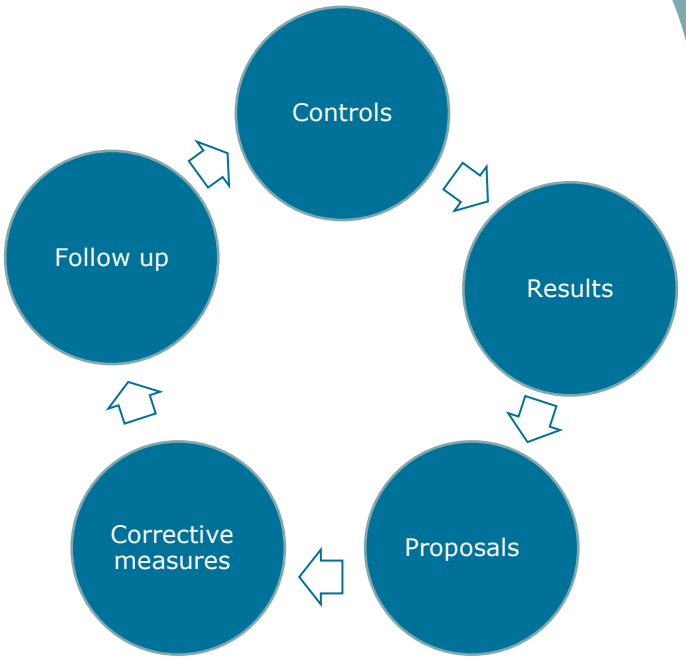
- **Article 42 (5) and (6)** of the amended CSSF Regulation N° 12-02:
  - reporting on a regular basis, or ad hoc if necessary, to the authorised management and, where appropriate, to the Board of Directors
  - at least once a year a summary report on activities and operations of the RC to the RR, authorised management and the Board of Directors, and where appropriate, the specialised committees.
- EBA guidelines on the role and responsibility of the AML/CFT Compliance Officer point 50.

RC report: purpose



- Provides the authorised management, the Board of Directors and the CSSF with an overview on RC's activities and operations.
- Allows the authorised management to take the necessary actions to correct findings and weaknesses, based on recommendations of the RC.
- Allows the RR to verify whether the defined AML/CFT framework has been implemented.

RC report: content



The RC report must contain:

- controls performed by the RC
- results of the controls
- description of corrective measures put in place
- proposal of corrective measures
- follow up on findings identified in previous report(s)

RC report: content

Sample testings according to compliance monitoring plan: results, corrective measures implemented, corrective measures proposed, follow-up e.g.:

- due diligence conducted on clients (including PEPs)
- periodic review of all clients according to their risk level (all performed, pending, reasons for delay)
- in case of AML/CFT outsourcing tasks, monitoring carried out
- treatment hits of name screening (pending hits)
- targeted financial sanction screening
- transaction monitoring
- data quality (database up to date)
- staff training on AML/CFT topics tailormade to business activity
- follow-up on findings of internal and external audits

EBA guidelines point 50
provides guidance content

cssf

Note: non-exhaustive list

RC report: content

- information on statistical data e.g.
  - number of SAR or STR
  - number of requests from the FIU, courts and law enforcement agencies
  - number of unusual transactions escalated to 2nd line of defense without filing STR and reason for not filing
  - number of reports to Ministry of Finance
  - number of blocked clients for ML/TF reasons
  - number of clients' relationships ceased by the entity due to AML/CFT concerns
  - number of reports to RBE

cssf

Note: non-exhaustive list

In case of questions, please send an email to:

aml.psf-sp@cssf.lu

Part I.

Legal persons and legal arrangements
ML/TF vertical risk assessment

1. Introduction and scope
2. Approach and methodology
3. Conclusions – main findings
4. Implications for professionals – results in practice

1. Introduction and scope (1/2)

- The **National risk assessment (NRA)** assessed the risk of misuse of its legal persons and legal arrangements as “High” (link)

- **FATF Recommendation 24 (R.24)** and its **interpretative note** on transparency and beneficial ownership of legal persons:

“countries should have mechanisms that […] assess the money laundering and terrorist financing risks associated with different types of legal persons created in the country, and take appropriate steps to manage and mitigate the risks that they identify” (link)

Note: following a 2022 update, the same is required too with regard to the risk associated with different types of foreign-created legal persons

- Several international reports and guidelines suggest that legal persons and legal arrangements are an attractive way for criminals to simulate and launder the proceeds of crime (link)

1. Introduction and scope (2/2)

- **All legal persons created in Luxembourg:**
  - ✓ Commercial companies:
    - SA, SARL, SARL-S, SNC, SCS, SCSpé, SAS, SCA, SCE, SCOOP, SCOOP SA, SE
  - ✓ Civil companies:
  - ✓ Non-profit organisations (NPOs):
    - *Associations sans but lucratif* (ASBLs)
    - Foundations
  - ✓ Other types of legal persons registered with the RCS:
    - Including, but not limited to *association d'assurance mutuelle, société d'épargne-pension à capital variable, groupement (européen) d'intérêt économique, association agricole, établissement public*
- **Domestic *fiducies*,** in view that the NRA specifically assessed domestic *fiducies* as a « very high » risk sub-sector.

2. Approach and methodology – level of analysis (1/4)

- Key references for this VRA: **FATF R.24 and its interpretative note** and **FATF Guidance on transparency and beneficial ownership**
- Some of these criteria are transversal (contextual) and more focused on the context/environment of Luxembourg companies, while others are more specific to the type of legal entity

R.24 criteria – illustrative exemples	Type of criteria
"Countries should take measures to prevent and mitigate the risk of the misuse of nominee shareholding and nominee directors […]" (Interpretative note 24.13)	Contextual ("Corporate")
"Countries should take measures to prevent and mitigate the risk of the misuse of bearer shares and bearer share warrants […]" (Interpretative note 24.12)	Specific

The analysis was carried out at two levels: contextual ("Corporate") and specific

2. Approach and methodology – inherent risk (2/4)

	Corporate risk ***Factor 1:*** *More relevant threats (NRA)*	**Entity-type specific risk** ***Factor 1:*** *Probability (likelihood)*
	Factor 2: *Inherent contextual vulnerabilities (circumstances or characteristics that affect Luxembourg's corporate environment and that could be exploited for ML/TF purposes)*	***Factor 2:*** *Inherent entity-type vulnerabilities (specific legal characteristics that could hamper transparency and thus facilitate anonymity)*
Obstacles to transparency (i.e. to obtaining BO information)	✓ The use of nominee arrangements ✓ The use of complex ownership and control structures	✓ The use of bearer shares ✓ Specific legal features that may foster complexity: o Transferability of shares o Shareholders = legal persons o Managers or directors = legal persons o (Public) availability of information on legal owners
Activity-based analysis		✓ The vulnerabilities of NPOs to be abused for TF purposes ✓ The use of legal persons as investment or asset holding vehicle

2. Approach and methodology – mitigating measures (3/4)

	Corporate risk	**Entity-type specific risk**
Controls by professionals subject to the 2004 AML/CFT Law	✓ The role of trust and company providers (TCSPs) as AML/CFT gatekeepers in the formation and throughout the life-cycle of legal persons and legal arrangements ✓ Financial institutions (FI) and designated nonfinancial business and professionals (DNFBPs)	✓ The role of notaries as AML/CFT gatekeepers ✓ Audit and control/oversight requirements
Information by the registries (RCS, RBE, RFT)	✓ Powers of the RCS registry to obtain and maintain basic information ✓ Capacity to obtain and maintain BO information through the BO registries (RBE, RFT)	✓ Filing of financial statements
Supervision and monitoring by authorities		✓ Supervision by different supervisory authorities of investment vehicles ✓ Controls by different Ministries for NPOs
International cooperation	✓ International cooperation	

2. Approach and methodology – mitigating measures (4/4)

Focus on the role of TCSPs as AML/CFT gatekeepers

→ **Professional obligations and registration requirements**

- Professionals must comply with their obligations under the 2004 AML/CFT Law when offering TCSP services. This helps mitigate the vulnerabilities for legal persons and legal arrangements in the Corporate risk, as TCSPs are able to **obtain basic information and BO information**. Furthermore, TCSPs are required to **monitor clients' transactions** based on materiality and risk, to ensure they are consistent with their knowledge of the customer, their business and risk profile, and sources of funds. TCSPs also have an obligation to **file suspicious transaction and activity reports to the CRF**.
- In addition to the licensing/qualification requirements for the types of professionals supervised by the CSSF, CAA, OEC, IRE and OAL/OAD, the 2004 AML/CFT Law requires them to **register as TCSP** with their respective supervisory authority or self-regulatory body (SRB), unless the supervisory authority has granted an exception.

→ **TCSPs play a significant role in in preventing ML/TF at two stages**

- Before the creation of legal persons and arrangements: TCSPs must perform **CDD controls** when providing support to the setup of legal persons and legal arrangements.
- During the life-cycle of legal persons and arrangements: TCSPs maintain a **long-term business relationship** with their corporate clients, allowing them to i) keep accurate CDD information and update it when necessary and, to ii) acquire an overall good knowledge of their clients, their activities, as well as their directors, managers, shareholders and BOs.

☞ This is particularly true when a single TCSP offers **multiple services** (e.g. domiciliation and directorship services) simultaneously to a client and it is particularly useful when monitoring the business relationship – i.e. for detecting ML/TF-related suspicious behaviour.

3. Conclusions – main findings (1/4)

Inherent contextual (« corporate ») risk:

Sociétés commerciales	*Sociétés civiles*	ASBLs	*Fondations*	Other legal persons	Legal arrangements

- Use of "*nominee arrangements": N/A in Luxembourg*
- **Main risk drivers for all categories**
  - ✓ High threat level applicable to legal persons and arrangements
- **Main risk drivers for commercial companies**
  - ✓ High share of corporate shareholders (i.e. commercial companies that are owned by other legal persons)
- **Main risk drivers for legal arrangements**
  - ✓ Presence of complex structures

3. Conclusions – main findings (2/4)

Contextual mitigating factors

Significant mitigation measures applicable to all categories of legal persons and legal arrangements

Residual contextual (« corporate ») risk

Sociétés commerciales	*Sociétés civiles*	ASBLs	*Fondations*	Other legal persons	Legal arrangements

3. Conclusions – main findings (3/4)

Inherent entity-type specific risk

SARL-S	SCOOP (SA); SC(Spé); SNC; *Société civile*	SAS; SE; SCA; ASBLs; *Fondations*	SA; SARL	*Fiducie*

- **Main risk drivers for SARL**
  - ✓ Higher likelihood of vulnerabilities being exploited
- **Main risk drivers for SA**
  - ✓ The entity can issue bearer shares (although this is regulated by the 2014 Share Registry Law)
  - ✓ Shares can be easily transferred to third parties
  - ✓ The legal owner is not mentioned in the articles of association
- **Main risk drivers for *fiducies***
  - ✓ Complex structures without ownership
  - ✓ Information on beneficial owners is not publicly available

3. Conclusions – main findings (4/4)

Entity-type mitigating mesures

SCSpé; *Société civile*; *Fiducie*	SCS; SNC; ASBL	SCOOP (SA); SA; SAS; SARL(-S); SCA	SCE; SE; *Fondation*

- **Mesures d'atténuation faibles pour SCSpé, Société civile et fiducie**
  - ✓ No need to be incorporated by notarial act
  - ✓ No specific audit and control requirements

Risque spécifique résiduel

SCOOP (SA); SCE; SARL-S; SE; SCS; SNC	SAS; SCA; SCSpé; *Société civile;* ASBL	SA; SARL	*Fiducie*

4. Implications for professionals – results in practice

This vertical risk assessment provides a set of criteria/questions that can be integrated by professionals in their own internal risk assessments and in the application of the risk-based approach (link for TCSPs)

For illustrative purposes (non-exhaustive list) :

- ✓ Was the legal person established by private or notarial act?
- ✓ What types of TCSPs are involved in the life-cycle of the legal person/legal arrangement?
- ✓ Who is registered as the beneficial owner with the RBE? The natural person who ultimately exercises control? A principal manager of the legal person?
- ✓ Who is the legal owner of the legal person? Is it a legal or a natural person?
- ✓ Is the information registered with the RCS and the RBE up to date? Is it consistent with the information available?
- ✓ When was the last update made in the RCS/RBE?
- ✓ Does the legal person/legal arrangement have a Luxembourg bank account?

Part II.

Terrorist financing
vertical risk assessment

1. Introduction
2. Approach and methodology
3. Inherent risk: threats and vulnerabilities
4. Mitigating factors and residual risk
5. Conclusions

1. Introduction

- **FATF recommendations** (link):
  - According to **R.1** on assessing risk and applying a risk based approach and its **interpretative note** *"Countries should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country […]"*
  - According to **R.8** on non-profit organisations (NPOs) and its **interpretative note** *"Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse […]"*

- The **2020 NRA** update (link) concludes that the threats of terrorism and terrorist financing (TF) are moderate overall. While the 2020 NRA covers both money laundering (ML) and TF, the **TF vertical risk assessment (TF VRA)** solely focuses on TF. Moreover, the TF VRA examined the FT risks posed to NPOs.

2. Approach and methodology (1/2)

- How to develop a TF risk assessment in a country with not known terrorist organisations operating on its soil
- How can the presence of the financial centre be taken into account?

Primary reference: FATF, *Terrorist financing assessment guidance,* 2019, §39 (link).

☞ Assessing TF risks in jurisdictions with financial centres and low domestic terrorism: Suitable for Luxembourg's particular situation.

The vertical risk assessment covers all three stages of TF:

Raising

Funds intended to be used to support a terrorist or a terrorist organisation are raised

Moving

Those funds are then moved to finance a terrorism-related activity

Using

Those funds are used to meet the needs of a terrorist or terrorist organisation

Starting point: **terrorism** (analysis of its context, the actors, their attacks and their financial needs)

→ **terrorist financing**

2. Approach and methodology (2/2)

1) Assessment of the different **kinds of terrorist actors** and categorized them according to their varying financial needs throughout the different stages of TF (i.e., raising, moving and using):
   - Small cells, lone actors and foreign terrorist fighters (FTFs): low financial needs.
   - International terrorist organisations and their wealthy sponsors: important financial requirements.

2) Analysis of the **terrorist attacks in certain regions to which Luxembourg is connected** through its geographical proximity (the European Union (EU) and the United Kingdom (UK)) or its financial centre (third countries):
   - Analysis of the TF exposure arising from lone actors and small cells operating within the EU and the UK (Islamic State of Iraq and the Levant (ISIL)-related and extreme right-wing terrorists): much smaller movements of funds channelled through specific services of the financial sub-sectors, such as retail banking and the money value and transfer services (MVTS) sector.
   - Analysis of TF risk arising from large flows of funds that may be channelled to or from foreign international terrorist organisations (e.g. ISIL) and transit through Luxembourg's financial centre.

3) A **sectoral analysis** is conducted in two steps (similar to the methodology used in the 2020 NRA, with specific adjustments):

1. INHERENT RISK assessment
(threats x vulnerabilities)

2. MITIGATING FACTORS assessment

RESIDUAL RISK

3. Inherent risk – threats (1/2)

European context

Terrorist attacks mainly perpetrated by **small cells or lone actors** related to ISIL (exception: certain attacks committed by extreme right-wing terrorists). Even though these attacks were quite numerous, their preparation and execution required **few financial means**.

Moreover, **FTFs** from EU Member States continue to be a source of concern.

Implications for the Luxembourg financial centre

→ **Main threat in relation to lone actors and small cells:**

- The exploitation and misuse of financial products offered by Luxembourg-based entities to collect, transfer and spend small amounts of money for TF purposes. This essentially concerns basic financial services offered to local and EU customers by retail and business banking, payment institutions (PI) and Electronic-money institutions (EMI).
- Luxembourg is exposed to this type of threat due to the number of entities providing such services (and not because of a higher risk of its basic services).

→ **Main threat in relation to FTFs entering or leaving conflict zones:**

- Withdrawal of cash from Luxembourg accounts through automated teller machines (ATMs) situated close to the conflict zones of Syria, Iran or Iraq.

☞ All Luxembourg financial institutions are fully regulated and supervised for anti-money laundering and countering terrorist financing (AML/CFT) purposes by the CSSF.

☞ The maturity and awareness for preventing TF of the financial sector is significant.

3. Inherent risk – threats (2/2)

Context in third countries with an active terrorist threat

While ISIL operates in the EU mainly through lone actors and small terrorist cells, it operates as a **terrorist organisation** in the safe havens provided by the vast deserted regions of the Sahara or the semi-deserted regions of the Sahel. From a quantitative point of view, the **TF needs** for ISIL and its affiliates in these regions are **very high**.

Implications for the Luxembourg financial centre

→**Main threats in relation to terrorist organisations and their wealthy sponsors:**

- Misuse of Luxembourg's financial centre to channel larger funds from or to international terrorist organisations established in regions particularly impacted by terrorism. This threat concerns the more sophisticated subsectors of the financial sector, mainly private banking and the investment sector.
- Raising funds (Luxembourg residents' donations to non-profit organisations (NPOs) carrying out development and humanitarian projects abroad) and moving funds (by sending funds to international terrorist organisations) by abusing Luxembourg's services commensurate with their higher financial needs).

☞ Luxembourg's exposure to these threats was assessed through the analysis of the financial, non-financial flows from and to a selection of relevant jurisdictions (and other variables).

☞ The analysed flows occur within intended and bilateral frameworks. The volume and nature of these flows did not reveal a material threat to Luxembourg's financial centre with respect to TF.

3. Inherent risk – vulnerabilities (1/6)

SECTORAL VULNERABILITIES:

Non-profit organisations (NPOs)

- Globally, NPOs carrying out development and humanitarian projects abroad are exposed at two key points of their operations: through the donations they receive and the destination of their funds.
- Although the globally observed typologies have not been detected in relation to Luxembourg NPOs developing projects abroad, this sub-sector remains highly vulnerable in view of the geography of their activities.

Retail and business banking sub-sectors

- Traditional banking products offered by retail and business banking (e.g. debit/credit cards, wire transfers, ATM withdrawals) make them vulnerable to TF by lone actors, small terrorist cells or FTFs that could misuse them to move funds cross-border.
- Luxembourg retail banking activities are focused on a local clientele.

According to a survey conducted by the CSSF and the ABBL on the retail banking activity (link), the majority of assets and liabilities are held by national residents (88%).

- Retail and business banks filed the highest number of STRs: 22 TFARs in 2020 (8 in 2019) and 4 TFTRs in 2020 (14 in 2019) (link).

3. Inherent risk– vulnerabilities (2/6)

Money value and transfer services (MVTS) sector

- Similar to retail and business banking, their products and activities allow easy access to fast and convenient cross-border transactions. This makes the sector vulnerable to being abused by FTFs, lone actors and small cells operating within the EU.
- The size and volume of transactions of Luxembourg's PI and EMI sub-sectors are large, while only a few agents/e-money distributors of PIs/EMIs, established in other EU Member States, operate in Luxembourg.

3. Inherent risk – vulnerabilities (3/6)

Private banking sub-sector

- Private banking's exposure to TF is driven by their size, international exposure, and nature of their clients (i.e. prevalence of big and potentially more sophisticated accounts).
- The financial threshold for entering into a business relationship and the close links with its clients (e.g. products are designed for a long-term relationship, use of relationship managers) make private banking unattractive to actors with low financial requirements.
- However, wealthy terrorism sponsors might enter into asset or wealth management agreements with Luxembourg private banks with a view to harbouring their assets even though the assets or wealth under management in Luxembourg might not be related directly to TF.

Investment sector

- As for the private banking subsector, the investment sector's exposure to TF appears more relevant for wealthy terrorism sponsors outside the EU than for lone actors or small terrorist cells operating within the EU. This is particularly true for the wealth and asset management subsector which typically caters to high net worth individuals.
- However, there is limited evidence that the investment sector is misused for TF purposes, as reflected by the very low number of TFARs and TFTRs filed. Notwithstanding this and similar to private banking, the sector's size is considered as a vulnerability factor.

3. Inherent risk– vulnerabilities (4/6)

☞ Within the private banking and investment sector, investment decisions may be performed on a discretionary basis (investment decisions are taken by the professional and not by the client).

Consequently, it is unlikely that funds are “moved” or “used” for TF purposes in the private banking and the investment sector.

In a similar vein, it is crucial to differentiate between the investments performed by the professional for the client, which are in principle inaccessible to the customer, and the client’s usage of those returns, unless they are reinvested.

3. Inherent risk – vulnerabilities (5/6)

CROSS-CUTTING VULNERABILITIES: CASH AND NEW TECHNOLOGIES

Cash

- Globally, cash is the most frequently observed mode of transportation for criminal purposes, including for TF.
- Turkey is considered a major transit hub for FTFs given its geographical location.
- The risks of TF resulting from the use of cash in Luxembourg must be taken into account by public and private entities.

☞ Luxembourg has not detected any terrorist groups operation on its soil and there is no known evidence for the collection of cash for TF purposes in Luxembourg.

☞ The analysis of ATM withdrawals in Turkey linked to accounts held with Luxembourg financial institutions near the Syrian, Iranian and Iraqi border shows that those were rather limited. Importantly, no evidence, was found to suggest that these amounts were linked to TF or FTFs.

3. Inherent risk – vulnerabilities (6/6)

New technologies

- According to a recent report by the **Royal United Services Institute** (link):
  - (i) New technologies (e.g. social media and crowdfunding, virtual assets) have not played a predominant role in the financing of most European terrorist attacks (i.e. those performed by lone actors and small cells). In most cases, attack-related items had been previously owned by the attacker or had been procured using cash or other common banking payment methods;
  - (ii) Terrorist groups have globally been observed to use virtual assets, donation-based crowdfunding, social media and payment services providers, especially in the "raising" and "moving" stages;
  - (iii) Overall, new technologies have been added to, rather than replaced, traditional financing methods.

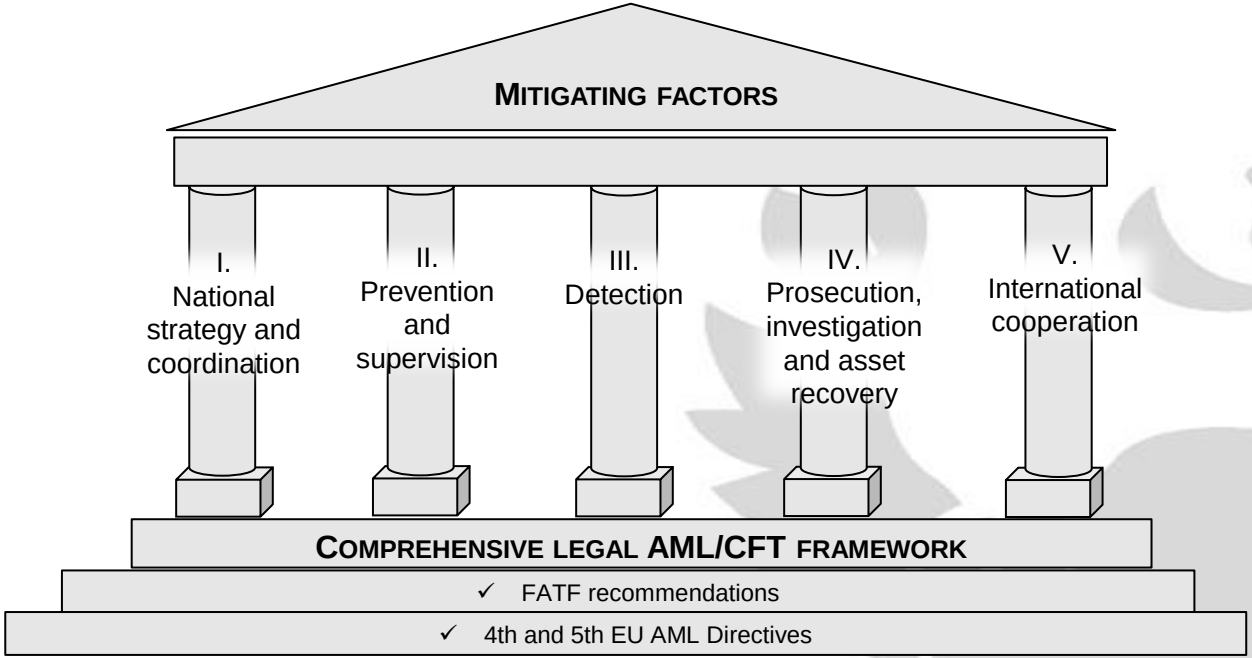
- Although the **2019 European Supranational risk assessment** (link) recognised the risks of virtual assets being misused to finance terrorism as emerging…
- … a more recent report from **Europo**l (2021) (link) states that the number of cases involving virtual assets for TF remains limited.
- As of 31 December 2021, there are 6 registered virtual asset service providers (VASP) in registered in Luxembourg. Six TFTRs/TFARs related to virtual assets or VASPs were reported to the CRF in 2020 and 29 in 2021. There is no evidence that Luxembourg VASPs are significantly exposed to TF.

4. Mitigating factors and residual risk

1. INHERENT RISK assessment
(threats x vulnerabilities)

2. MITIGATING FACTORS assessment

RESIDUAL RISK



4. Mitigating factors and residual risk

Sector	Subsector	Inherent TF risk		Residual TF risk
Banks	Private banking	**Medium**		**Low**
	Retail and business banks	**High**		**Medium**
Investment sector	Wealth and asset managers	**Medium**		**Low**
	Collective investments	**Medium**		**Low**
Money value and transfer services	Payment institutions (PI) E-money institutions (EMI) Agents and e-money distributors acting on behalf of PI/EMIs established in other European Member States	**High**	*Impact of mitigating factors*	**Medium**
NPOs carrying out development and humanitarian projects abroad	NPOs (*Associations sans but lucratif* (ASBLs) and *fondations*) carrying out development and humanitarian projects abroad	**High**		**High**

5. Conclusions (1/2)

To conclude, the following table depicts Luxembourg's TF residual risk at the three stages of TF: raising, moving and using funds for terrorist purposes for the different assessed (sub)sectors:

	Raising	**Moving**	**Using**
Retail and business banking	Small cells, lone actors and FTFs may raise legitimate funds such as salaries, social benefits, non-paid-off customer loans, overdrafts	Basic financial services (e.g. wire transfers/ ATM withdrawals) might be misused to move funds intended for TF purposes to small cells, lone actors and FTFs	Small cells, lone actors and FTFs may use funds to commit terrorist acts
Private banking and Investment sector	Relevant for wealthy terrorism sponsors outside the EU	Discretionary asset management is not suitable for moving funds for TF purposes. Funds managed by the asset manager under a discretionary contract are inaccessible to the customer. Generated returns that are no longer subject to discretionary management may be transferred to terrorists or terrorist organisations	Not applicable as long as the funds are under discretionary management This does not exclude the investment sector from performing (enhanced) due diligence on investment projects in regions impacted by terrorism and companies operating in such regions

5. Conclusions (2/2)

(…)	Raising	Moving	Using
MVTS	Small cells, lone actors and FTFs may abuse MVTS providers to raise funds for TF purposes (including payments related to crowdfunding services)	MVTS might be misused to move funds intended for TF purposes to small cells, lone actors and FTFs	Small cells, lone actors and FTFs may use funds to commit terrorist acts
NPOs carrying out development and humanitarian projects abroad	NPOs may raise funds (advertently or inadvertently) for TF purposes	Some high-risk jurisdictions have limited access to the international correspondent banking systems and some NPOs carrying out development and humanitarian projects abroad may be tempted to use informal or non-regulated channels (e.g. *Hawala* or other service providers) to transfer funds to those jurisdictions No evidence of *Hawala* or other service providers operating in Luxembourg	Not applicable, except for NPOs raising funds advertently for TF purposes

Thank you for your attention!

PARQUET GÉNÉRAL
DU GRAND-DUCHÉ DE LUXEMBOURG
CRF - Cellule de renseignement financier

INSIGHTS FROM THE FIU LUXEMBOURG FOR SPECIALIZED PROFESSIONALS OF THE FINANCIAL SECTOR

2023 AML/CFT Conference dedicated to Specialised Professionals of the Financial Sector

30 January 2023

AGENDA

About Us
CRF - FIU Luxembourg in a nutshell

Key figures 2022
With a focus on specialized PSFs

Fight against ML / TF
Case study

Best practice guide
Reporting suspicious activity and / or transactions to the CRF - FIU

Q&A

PARQUET GÉNÉRAL
DU GRAND-DUCHÉ DE LUXEMBOURG
CRF - Cellule de renseignement financier

CRF - FIU LUXEMBOURG

IN A NUTSHELL

FIU Luxembourg

In a nutshell

Judicial FIU

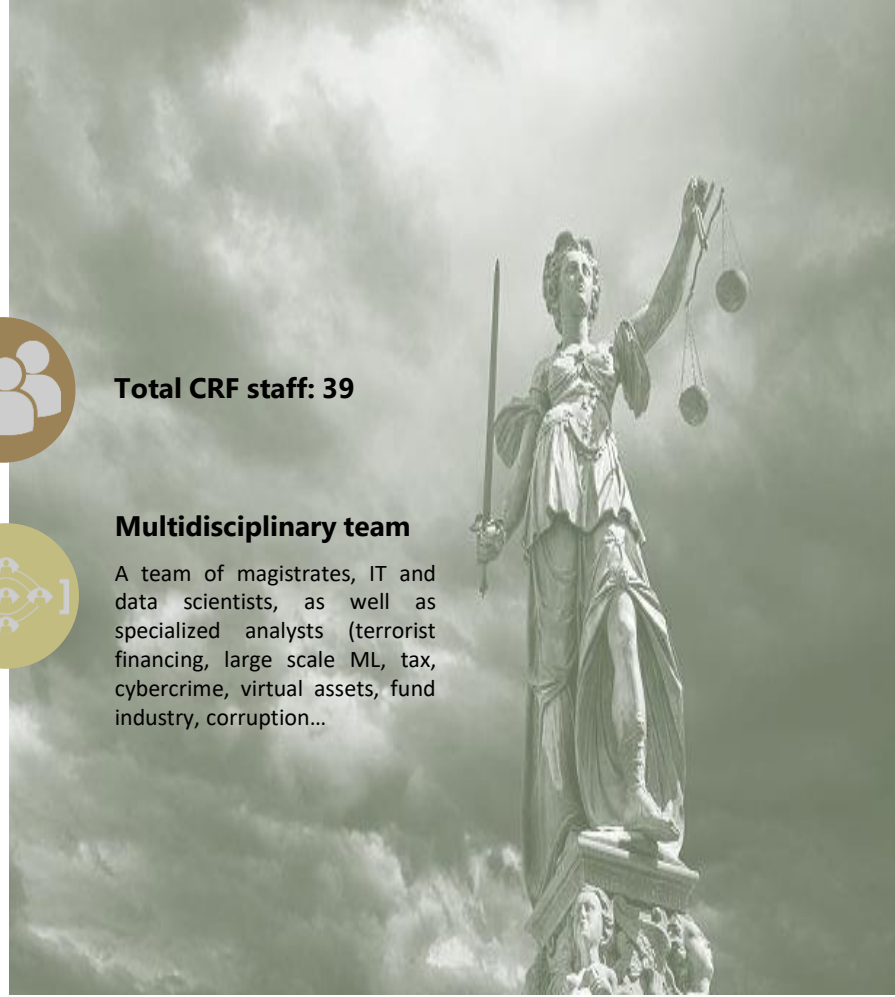
Operationally independent and autonomous

Under the administrative supervision of the General prosecutor

Total CRF staff: 39

Multidisciplinary team

A team of magistrates, IT and data scientists, as well as specialized analysts (terrorist financing, large scale ML, tax, cybercrime, virtual assets, fund industry, corruption…



FIU Luxembourg

Key figures of the year 2022

53 391

Suspicious activity reports received

3 677

Case files on suspicious transactions

2 825

Outgoing foreign requests / spontaneous disseminations

791

Incoming foreign requests / spontaneous disseminations

~ EUR 300 mio

Currently frozen

100%

Completely digital

Top 5

predicate offenses

- Fraud
- Criminal tax offenses
- Counterfeiting & product piracy
- Money laundering

Top 5

international cooperation – outgoing

Top 5

international cooperation – incoming

305

Disseminations to national judicial authorities and AML/CFT competent authorities

PARQUET GÉNÉRAL
DU GRAND-DUCHÉ DE LUXEMBOURG
CRF - Cellule de renseignement financier

CRF - FIU LUXEMBOURG

KEY FIGURES 2022
FOCUS ON SPECIALIZED PFS

Disclaimer

Beware of the statistics in this presentation!

A reporting entity can play different roles,

- *Registrar agent*
- *Corporate domiciliation agent*
- *Family Office*
- *Professional providing company incorporation and management services*

However, goAML does not allow to specify multiple roles.

Therefore, statistics may give an incomplete picture of the level of cooperation with a specific sector.

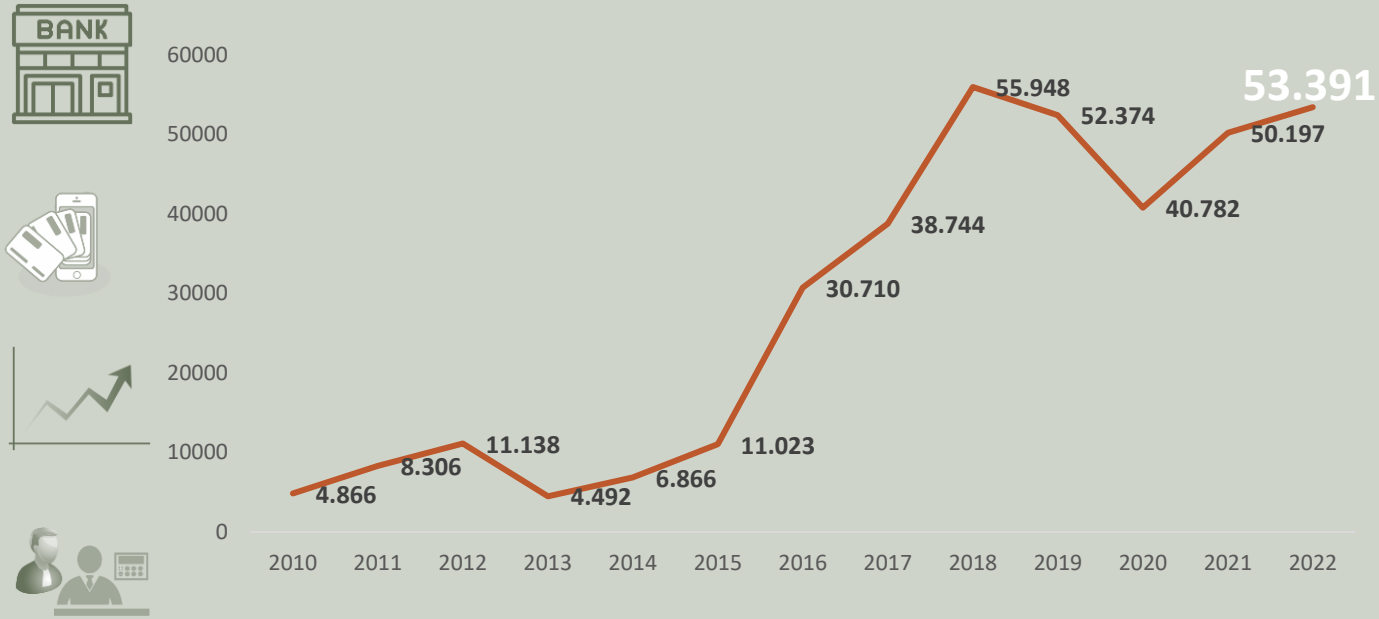
Number of Specialised PFSs registered in goAML

Statistics 2022

	Registered in goAML (2023 ytd)
Article 25. PFS / Registrar agents	23
Article 26. PFS / Professional depositaries of financial instruments	2
Article 26.-1. PFS / Professional depositaries of assets other than financial instruments	2
Article 27. PFS / Operators of a regulated market authorised in Luxembourg	2
Article 28-2. PFS / Currenency exchange dealers	0
Article 28-3. PFS / Debt recovery	1
Article 28-4. PFS / Professionals performing lending operations	6
Article 28-5. PFS / Professionals performing securities lending	0
Article 28-6. PFS / Family Offices	11
Article 28-7. PFS / Mutual savings fund administrators	1
Article 28-9. PFS / Corporate domiciliation agents	61
Article 28-10. PFS / Professionals providing company incorporation and management services	10

Total number of suspicious transactions reports filed to the CRF

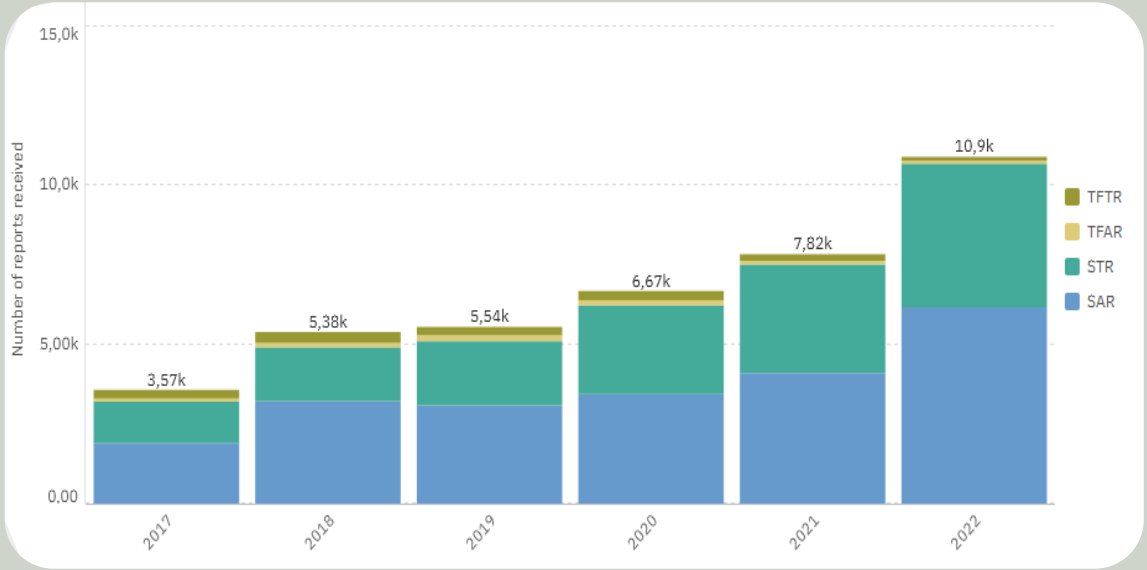
Statistics 2022



Total number of suspicious transactions reports filed to the CRF

Statistics 2022

Number of spontaneous transaction reports received
(excluding reports received from entities operating online)



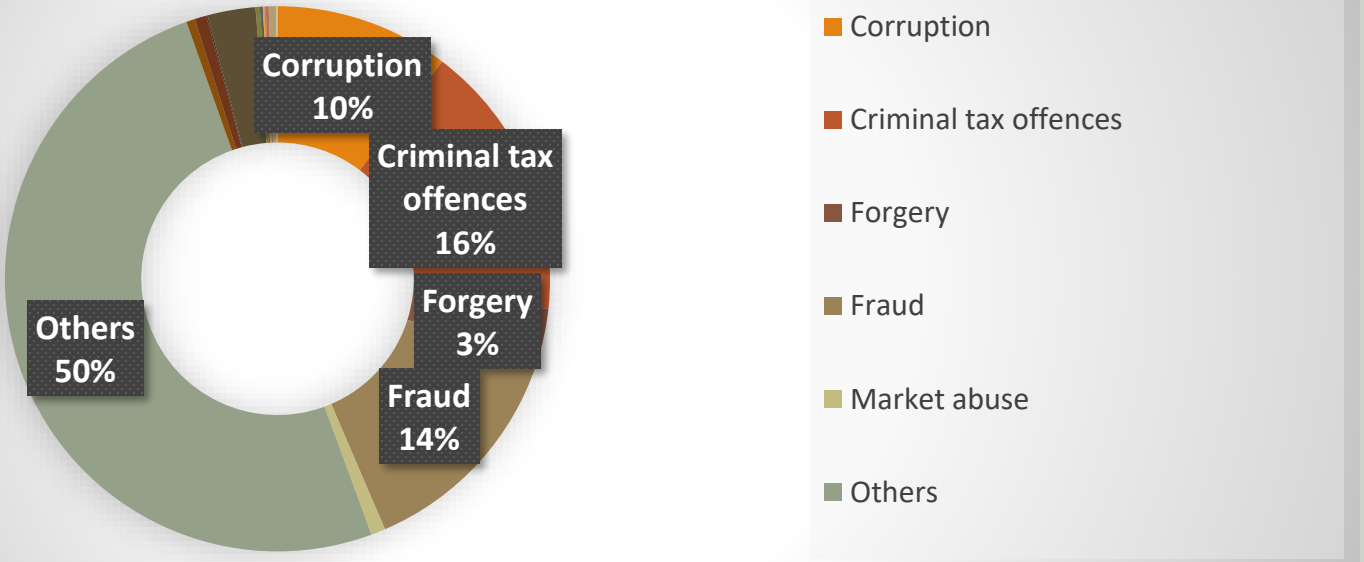
Total number of suspicious transactions reports filed by specialised PFSs

Statistics 2022

	2017	2018	2019	2020	2021	2022	TOTAL
Article 25. PFS / Registrar agents	29	48	36	15	18	22	168
Article 26. PFS / Professional depositaries of financial instruments					1	1	2
Article 26.-1. PFS / Professional depositaries of assets other than financial instruments				1	1		2
Article 27. PFS / Operators of a regulated market authorized in Luxembourg			1	1	1	4	7
Article 28-2. PFS / Currency exchange dealers							0
Article 28-3. PFS / Debt recovery	4			20	15	1	40
Article 28-4. PFS / Professionals performing lending operations	2	2	2	2	1		9
Article 28-5. PFS / Professionals performing securities lending							0
Article 28-6. PFS / Family Offices		17	5	3		1	26
Article 28-7. PFS / Mutual savings fund administrators							0
Article 28-9. PFS / Corporate domiciliation agents	134	157	171	170	121	113	866
Article 28-10. PFS / Professionals providing company incorporation and management services	2	6	3	3	10	8	32
Grand Total	171	230	218	215	168	150	1152

Suspicious transactions reports filed by specialised PFSs
Top 5 Predicate offenses

Statistics 2022



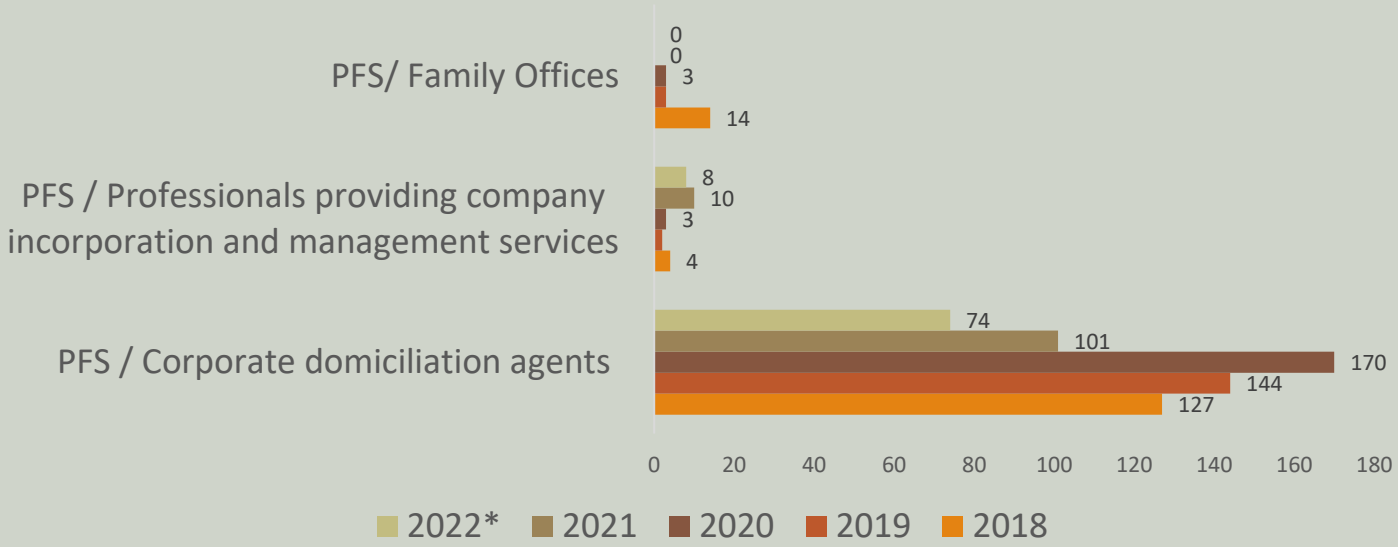
Suspicious transactions reports filed by specialised PFSs
Top 5 Indicators

Statistics 2022

1. Open source indications and information
2. Reluctance to provide KYC / KYT documentation
3. Unusual behavior of the customer
4. Offshore based companies
5. Suspicious transaction pattern

Focus on the number of TCSP related SARs/STRs filed by specialized PFS

Statistics 2022

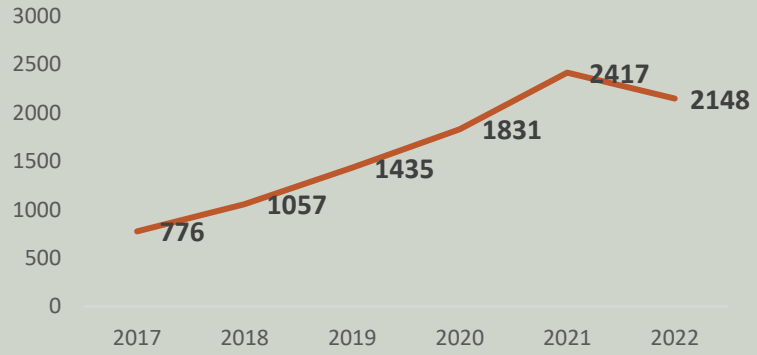


* Figures until 11/2022

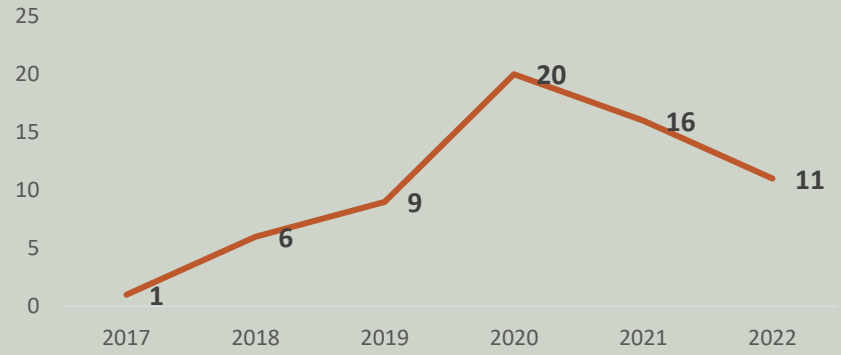
Number of requests for information issued by the CRF

Statistics 2022

Total number of requests for information



Number of requests for information sent to specialised PFSs



Typologies and trends observed in 2022

Misuse of legal persons and legal arrangement for ML/TF purposes

Beneficial owner concealment

Misuse of the real estate sector for ML/TF purposes

"Professional Money Launderers" and the concept "crime as a service"

Increased use of "money mules"

Cybercrime, use of virtual assets, anonymization tools, etc.

PARQUET GÉNÉRAL
DU GRAND-DUCHÉ DE LUXEMBOURG
CRF - Cellule de renseignement financier

THE FIGHT AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

BEST PRACTICE GUIDE

Best practice guide

Much more important than the quantity of reports submitted is the **quality and relevance** of the information provided.

1. Defensive filing
2. Incomplete filing
3. « tick the box » approach

Is it sufficient to provide supporting documents?

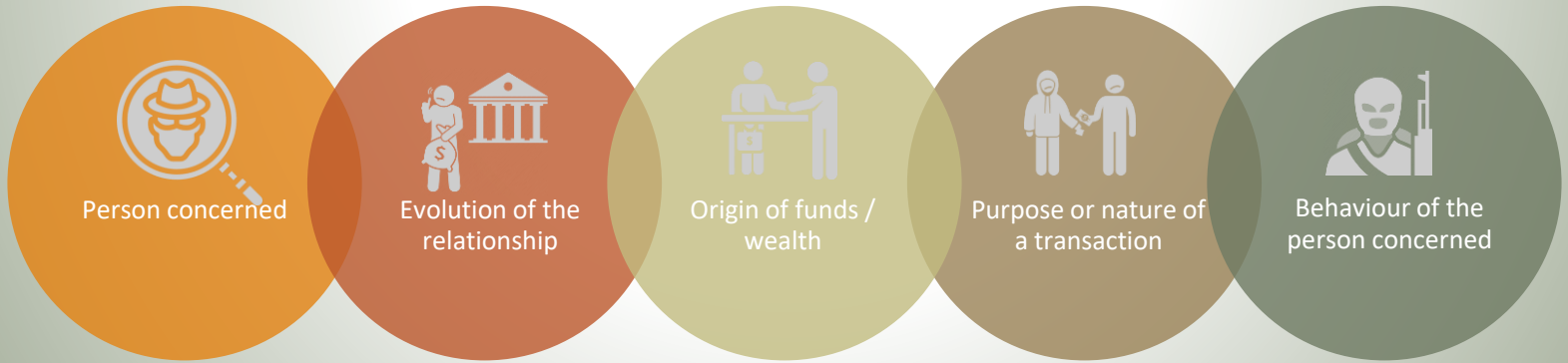
No, the relevant questions are:

- How were the funds generated?
- What economic activity generated the funds?
- The economic sense behind a complex legal set-up of companies.

Focus on doubt vs suspicion vs evidence

Pursuant to Article 5 (1) a) of the amended Law of 12 November 2004 on the fight against money laundering and terrorist financing, professionals are obliged to inform the CRF without delay, on their own initiative, when they **know, suspect or have reasonable grounds to suspect** that money laundering, an associated predicate offence or terrorist financing is in progress, has taken place or has been attempted.

Doubts or suspicions may be raised regarding:



Doubt vs suspicion

Doubt

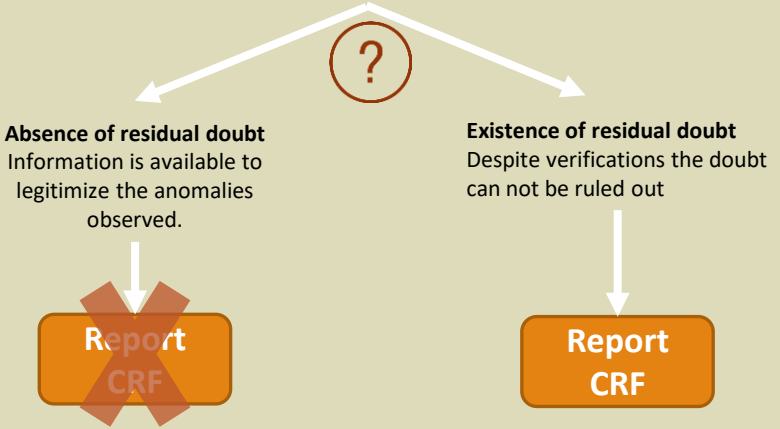
Doubt often arises from "negative" information based on **open source information*** *(adverse media, sanction or compliance / watch lists, etc.)* or is related to the **behavior** of the **person concerned** *(+ forged supporting documents)*

Doubt may arise from an **atypical transaction / operation** or from a transaction that deviates either from the standard or from the client's own **pattern of transactions** *(i.e. transactional flows are disproportionate to the reported sources of income (Mule))*

Indicators based on a **transaction's amount** or **frequency, beneficiary** or **its atypical nature**.

Suspicion

Verification of doubt: is there a legitime explanation for the observations made (i.e. KYC, KYT, etc.) ?



suspicion arises when doubt cannot be removed

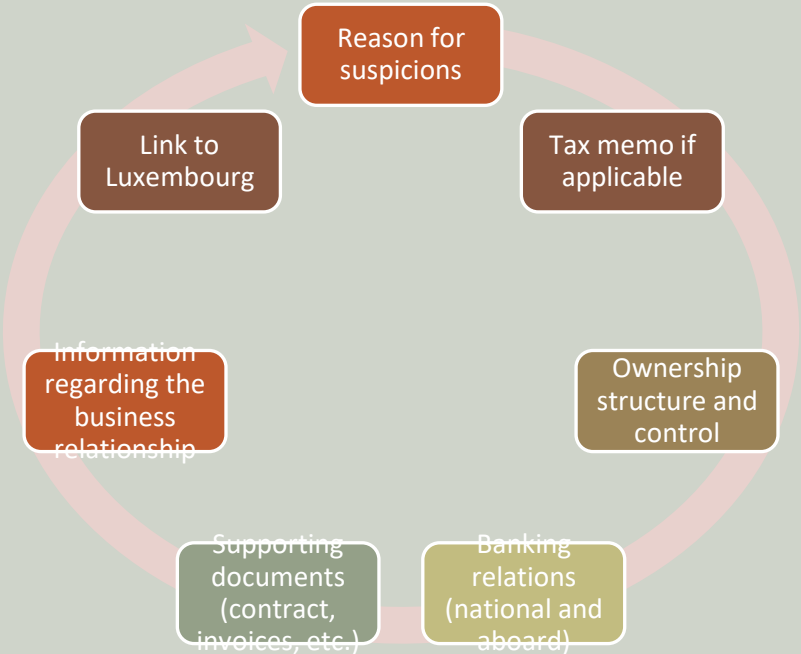
* *Pandora Papers, Panama Papers, Openlux, etc.*

Best practice guide

Importance of providing <u>structured data</u>. Please provide in goAML **exhaustive information**, involved persons, entities (incorporation nbr, legal form, etc.), accounts, etc. → *Important for strategic and typology analyses conducted by the CRF*

New "Feedback form". Direct feedback given by the CRF on the report quality.

Try to be as exhaustive and comprehensive as possible. For example: *Adverse media has been published on XYZ. Include information about the relationship, possible additional information (is there a link between the publication and the client?), suspicious transactions, banking relationships in Luxembourg and abroad, etc.*



Best practice guide

Report: refusal to enter into a business relationship

- Even if the decision has been taken not to enter into a relationship with a prospect because of ML/TF suspicions, share them with the CRF.

Urgent Requests for information issued by the CRF

- Importance of answering to urgent requests for information without delay or at least to notify the CRF in case of additional time needed
- If the requested information / documents are not available, please notify the CRF, to clarify if the documents should be requested or not

Freeze orders issued by the CRF: No Tipping-off

Thank you for your attention

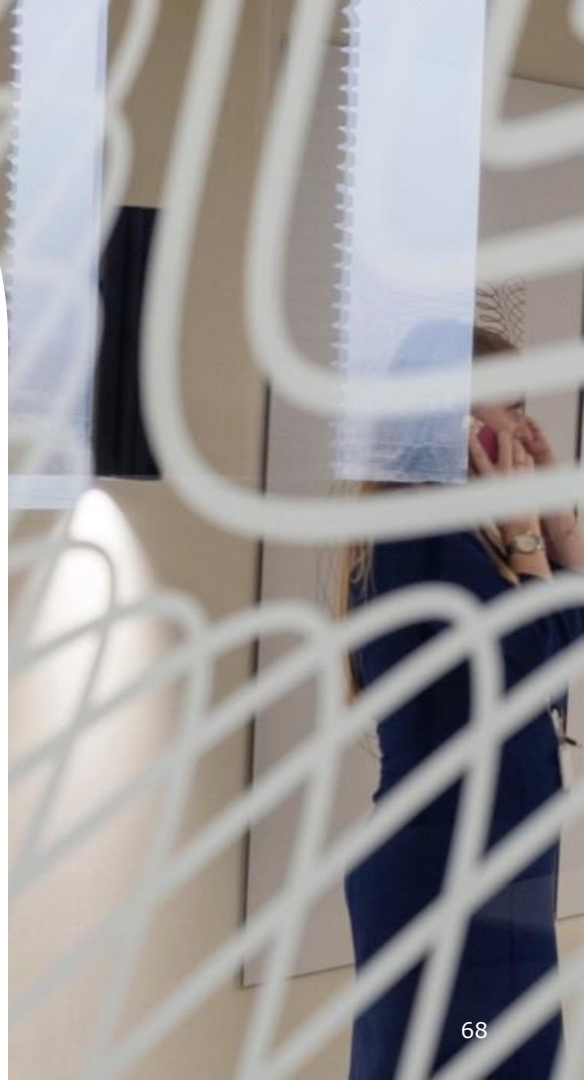
Questions

AML/CFT
Expert Working Group for Specialised PFS

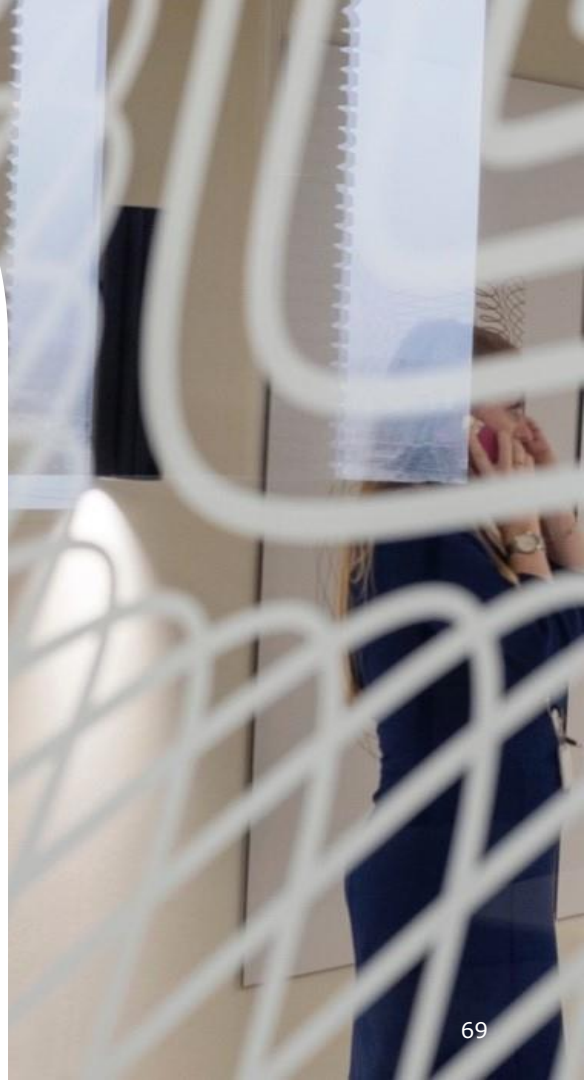
cssf
Commission de Surveillance du Secteur Financier

AML/CFT: EXPERT WORKING GROUP FOR SPECIALISED PFS

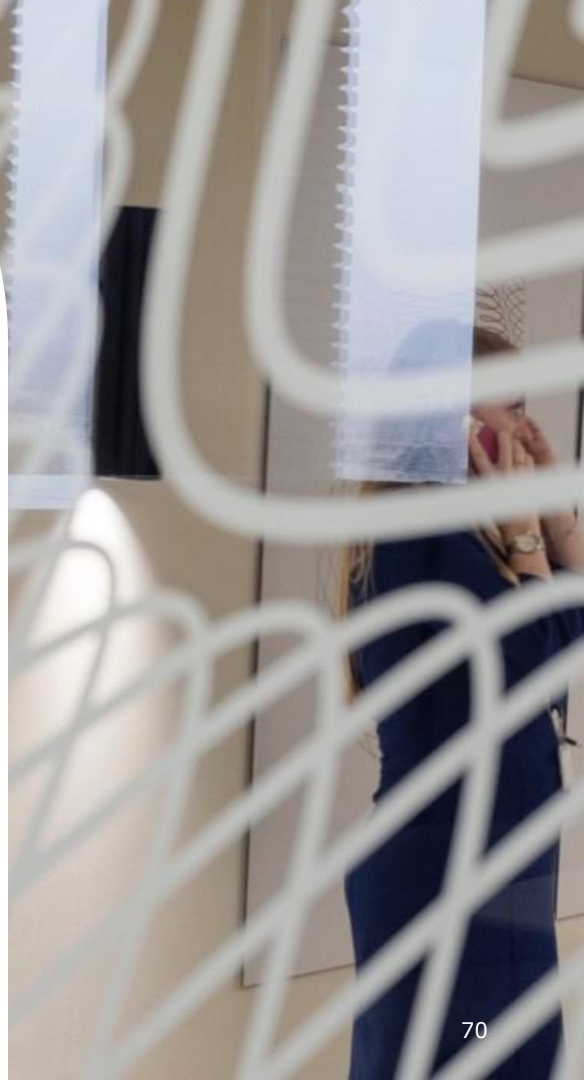
- On **20 July 2020**, the CSSF published the first Sub-Sector Risk Assessment on Trust and Company Service Providers activities in Luxembourg.
- It is a **sectorial analysis** which complements the updated National Risk Assessment.
- **ML/FT threats and vulnerabilities** are analysed together with **mitigation factors**.



- Specialised PFS are expected to take the findings of the SSRA (in addition to the ones of the updated NRA and the Supra National Risk Assessment) into account in their **AML/CFT frameworks.**
- The aim of the SSRA is to help Specialised PFS to have a **better understanding of their ML/FT risks.**
- Both NRA and SSRA concluded that the **inherent ML/FT risks are high** and the residual risks, after implementation of mitigation factors, **medium-high**.

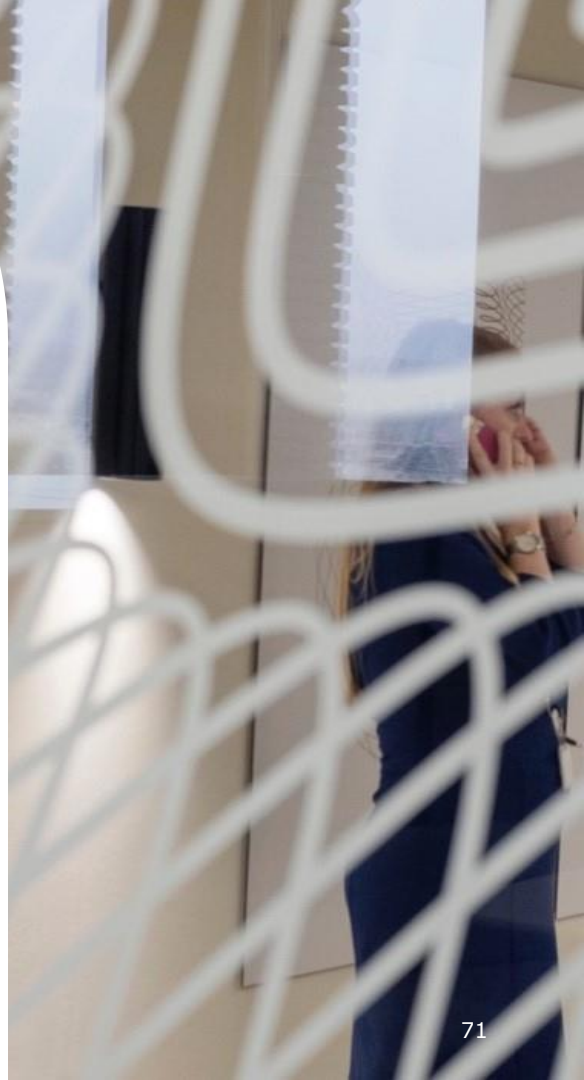


- **October 2019:** Creation of Expert Working Groups **AML OPC** and **Private Banking**
- **Press release 22/23**: In order to further strengthen their collaboration in the fight against ML/FT, the Luxembourg Bankers' Association (ABBL), the CRF and the CSSF have signed a Public Private Partnership on 13 September 2022.
- **October 2022**: creation of a permanent joint **Expert Working Group on ML/FT risks for Specialised PFS**.

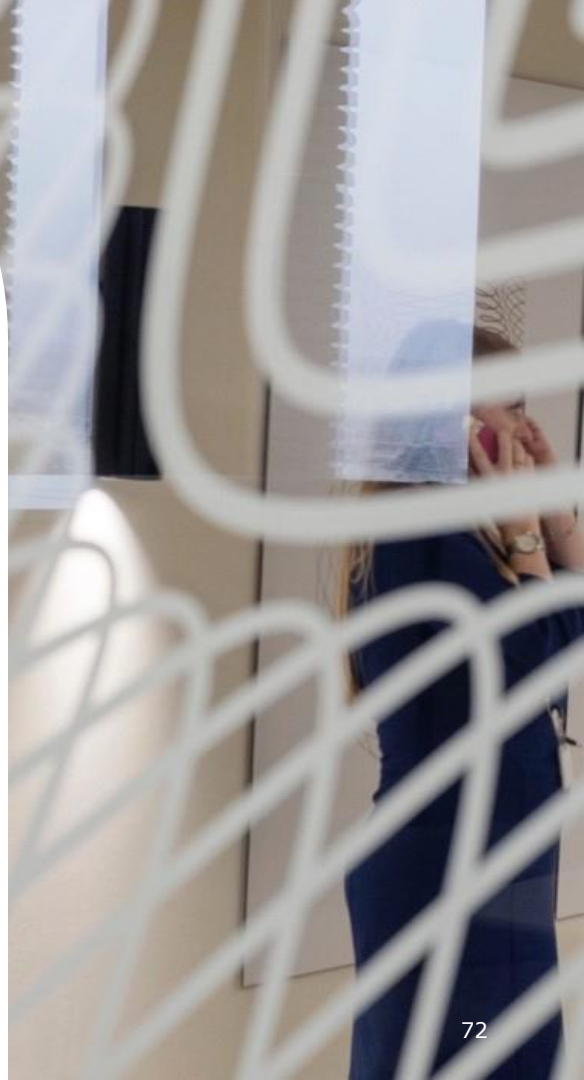


- **Members of the EWG** are:

- Luxembourg Alternative Administrators Association **(L3A)**
- Luxembourg Private Equity & Venture Capital Association **(LPEA)**
- Luxembourg Association of Family Offices **(LAFO)**
- Association of Luxembourg Compliance Officers **(ALCO)**
- Cellule de Renseignement Financier **(CRF)**

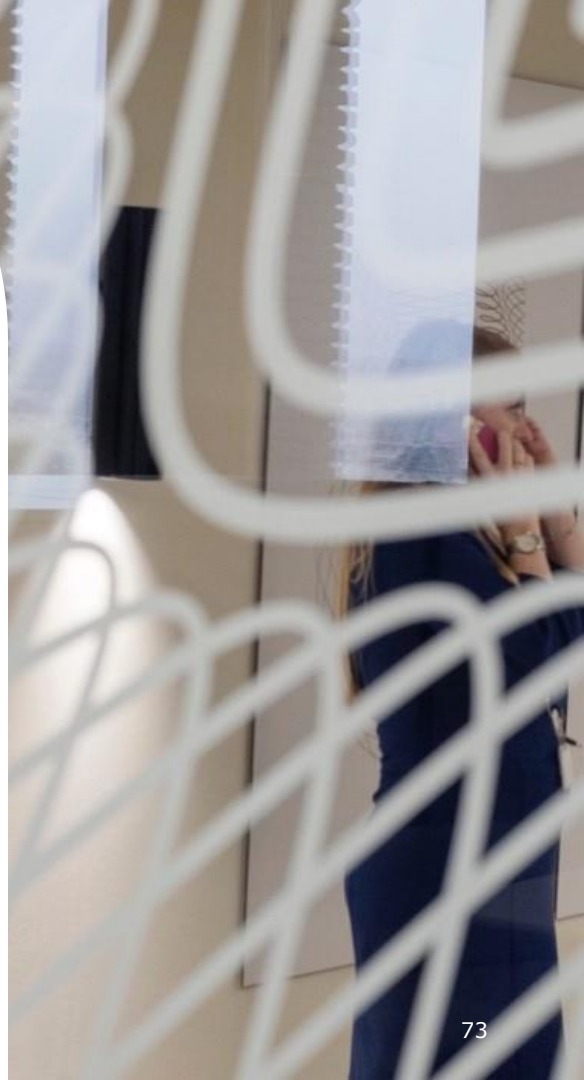


- The fight against ML/TF requires an **integrated approach** in which public authorities and industry representatives **pool their knowledge and skills** to prevent, detect and combat these crimes together. Such a public-private dialogue **helps providing clarity on risks** related to specific activities, typologies of crimes, regulatory expectations, and also aims at identifying specific areas or issues where more **regulatory guidance** is needed.

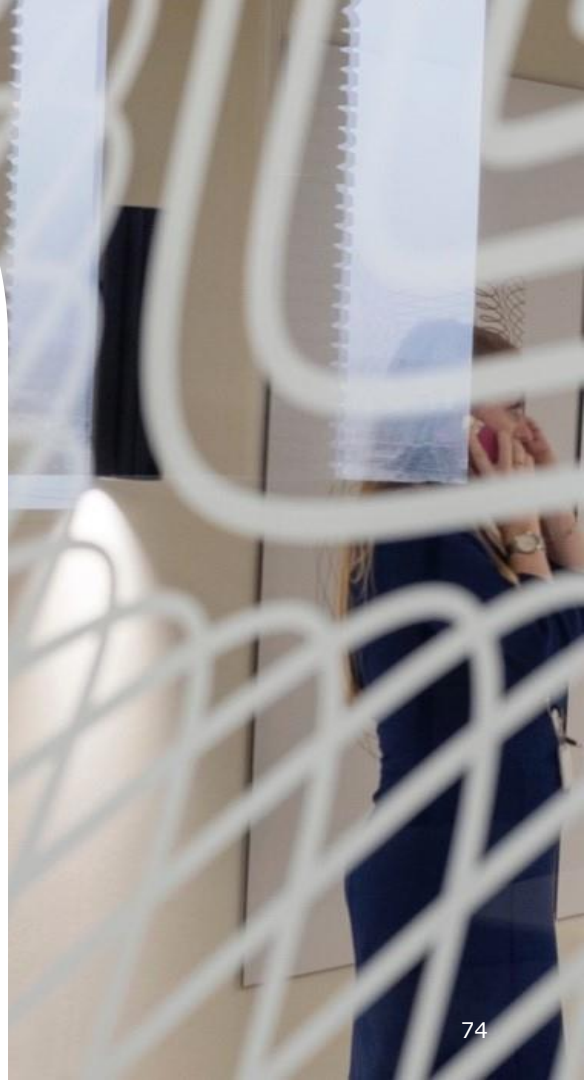


- The **first meeting of the EWG** took place on 17 October 2022 and meetings continue on a **regular schedule** to discuss topics that are relevant to ML/FT prevention by Specialised PFS performing TCSP activities.
- **Agenda:**

- Approval of the "**Terms of Reference**" of the EWG
- Presentation of the **L3A Charter** on minimum standards of AML/CFT procedures of Specialised PFS

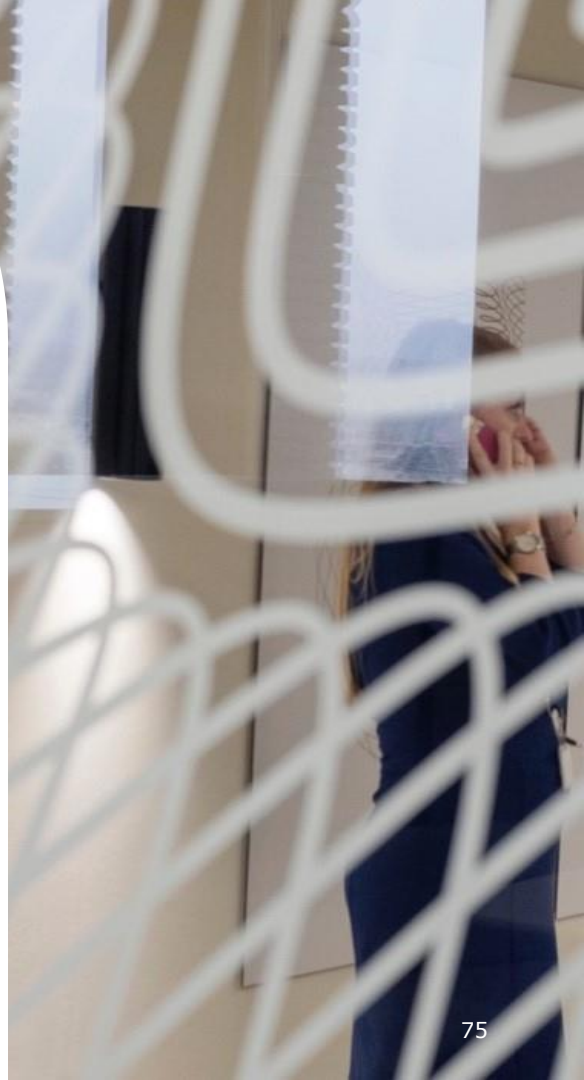


- **Review of the SSRA on TCSP** during 2023.
- **Vertical Risk Assessment on legal persons and legal arrangements** (23 February 2022)
- **Vertical Risk Assessment on Terrorist Financing** (May 2022)
- **2022 Supra National Report** of the European Commission on the assessment of the risk of ML and TF, published on 7 December 2022 on the CSSF website



2022 SNRA

- The Commission published its first supranational risk assessment (SNRA) in 2017 and the second in 2019.
- The SNRA provides a comprehensive **mapping of risks** on all relevant areas, as well as the necessary **recommendations to counter them**.
- Due account has been taken of **national risk assessments (NRAs)** produced by the Member States.
- The Commission has carried out a **broad consultation exercise** involving as many relevant stakeholders as possible.



cssf

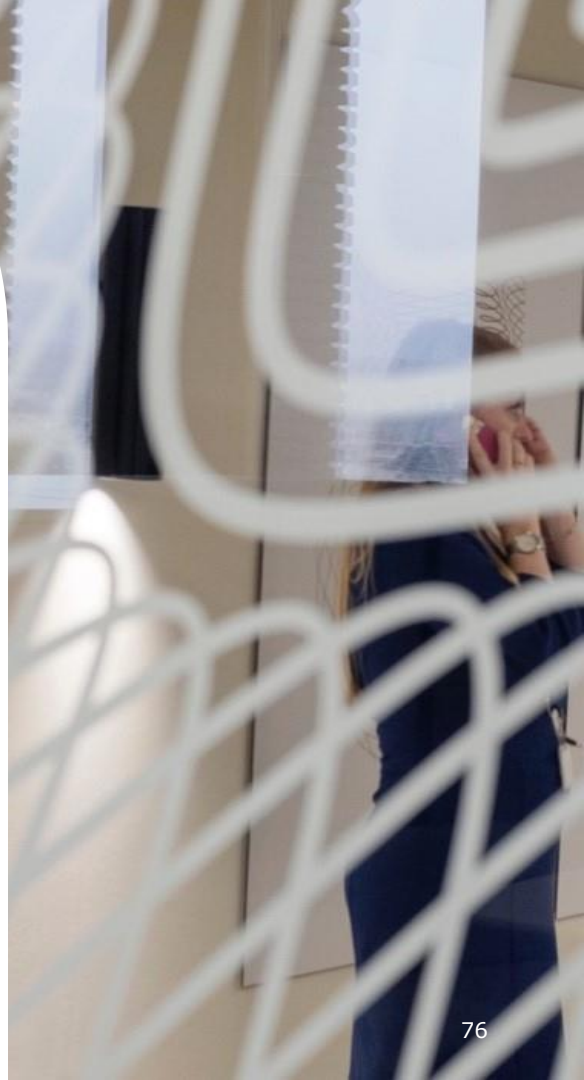
- The SNRA took into account:

- The **impact of the COVID-19 pandemic**.

- The **Russian war of aggression against Ukraine**.

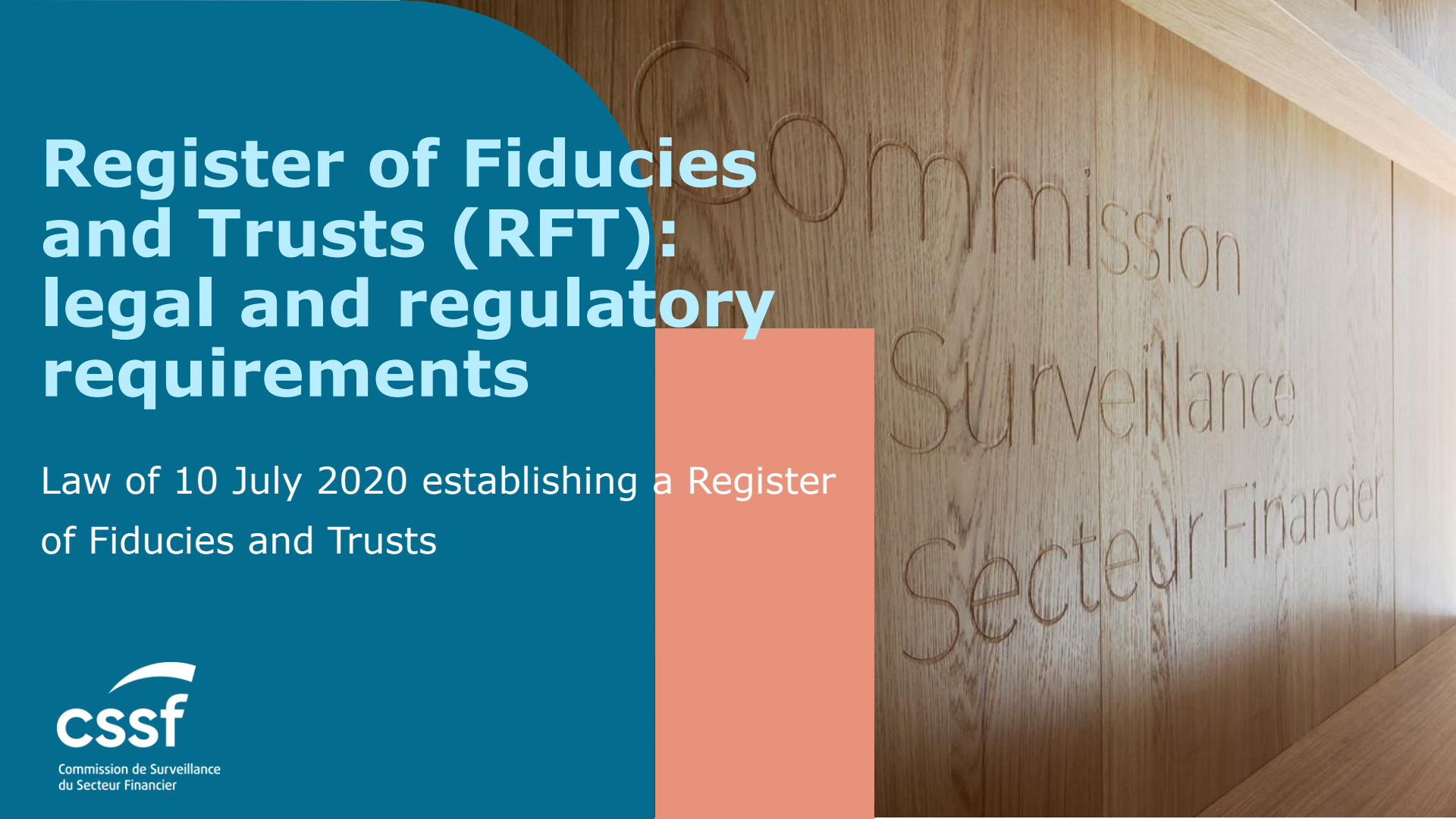
- **Main risks covered** by the SNRA:

- Cash and cash-like assets
- Financial sector
- Non-financial sector and products
- Collection and transfer of funds through Non-Profit Organisations (NPOs)
- Professional sports



Register of Fiducies and Trusts (RFT): legal and regulatory requirements

Law of 10 July 2020 establishing a Register of Fiducies and Trusts



cssf
Commission de Surveillance du Secteur Financier

Legal requirements

- **Article 2: (1)** Trustees and fiduciaires shall obtain and keep, (…) **information on the beneficial owners** of any express trust administered in the Grand Duchy of Luxembourg and of any fiducie for which they act as trustee or fiduciaire.
- **Article 7**: The CSSF (…) shall monitor the **compliance with the obligations** provided for in this chapter by the persons for whom they are respectively responsible for ensuring compliance with the professional obligations, in the exercise of their professional activity, relating to the fight against ML/TF.

Chapter 4 Registration and conservation of information in the RFT

- **Article 13: (1)** Every fiducie and every express trust of which a trustee or fiduciaire is established or resides in the Grand Duchy of Luxembourg shall be **registered** with the RFT.
- **Article 14**: **Data to be registered** with the RFT.
- **Article 16: (1)** The **AED** is responsible for the safeguarding, administrative management and provision of the information recorded on fiducies and express trusts in accordance with the provisions of the law.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Administration de l'enregistrement,
des domaines et de la TVA

- **Article 19:** Any person having access to the information recorded in the Register of Fiducies and Trusts shall **promptly report** to AED **any discrepancies** that he or she encounters between the information on beneficial owners available in the Register of Fiducies and Trusts and the information on beneficial owners available to him or her.

cssf

cssf
Commission de Surveillance
du Secteur Financier

Thank you
for your attention!