2026 AML/CFT Conference

Dedicated to Specialised Professionals of the Financial Sector

26 January 2026

cssf
Commission de Surveillance du Secteur Financier

Rules of the conference

- Cameras, microphones and chat function are deactivated
- No recording (audio, video, …)
- Presentation slides will be published on CSSF website
- This conference cannot replace the regular AML/CFT trainings
- No certificate of attendance will be provided

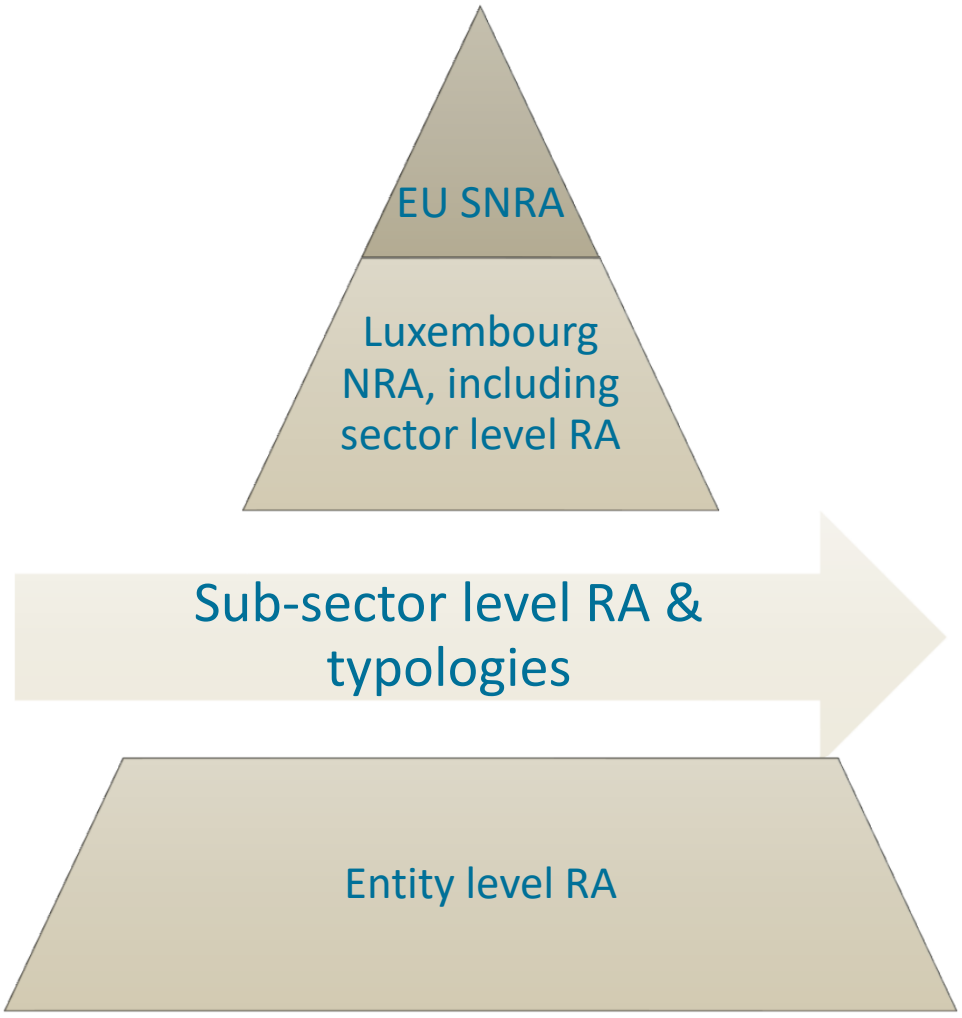
Agenda

- Foreword
- Update Sub-Sector Risk Assessment Specialised PFS providing corporate services
- Thematic review TF
- Insights from the FIU for Specialised PFS
- 2025 ML National Risk Assessment
- Conclusion

SSRA on TSCPs

Specialised PFS providing corporate services

(Trust and Company Service Providers)



Why a SSRA on TCSPs?

Objectives of the SSRA:

- **Better understanding of the risk** in relation to TCSP activities
- **Resource for the supervision** by the CSSF
- **Guidance to the industry for the assessment of the risks** of TSCP activities
- **Promotion of understanding of ML/TF risks** and **AML/CFT obligations** in the industry
- **Public-private partnership**

cssf

Sector and sub-sector risk assessment approach

Step	Description
1. Define risk assessment scope and methodology	**CSSF defined the scope of the report**, **including the methodology** (e.g. risk factors, risk scoring) **and workplan** (e.g. timelines, key stakeholders)**.** This includes determining the taxonomy (e.g. the types of products/activities within the sector that should be assessed)
2. Perform desk-based research	**CSSF drafted the preliminary report** based on quantitative and qualitative information gathered through desk-based research from: (i) international sources (e.g. FATF RBA); (ii) other domestic sources (e.g. CRF reports), (iii) internal CSSF data collected via its supervisory activities, (iv) expert input (see below); (v) and information provided by the private sector (e.g. via AML/CFT questionnaires)
3. Gather input from experts	**An expert panel**, composed of CSSF and external experts, **reviewed the findings** and provided feedback
4. Consolidate findings in a report	**CSSF consolidated findings into two reports**: an internal version and a publishable version
5. Gather feedback	**CSSF presented the draft publishable report** to the private sector to gather feedback. For Collective Investments and Private Banking this was during Expert Working Group (EWG) meetings; for TCSPs this was directly with the relevant industry association (L3A) (see Core Issue 3.6 for details)
6. Publish report and raise awareness	**CSSF published the final report** and raised awareness via press releases, newsletters, and conference presentations

cssf

The SSRA provides for the link between the NRA and entity-level risk assessments. It fulfils multiple objectives

- **Reflect the CSSF's own understanding** of specific ML/TF risks in the sub-sector;
- Further **improve the CSSF supervisory activities** and sub-sector specific supervisory strategy, where relevant;
- **Act as an input** into CSSF's entity-level risk assessments;
- **Serve as a resource** for the industry in informing their own ML/TF risk assessments;
- **Promote the understanding** of ML/TF risks and AML/CFT obligations in the industry; and
- **Support public-private interaction**.

Definition of TCSP

The 2004 AML/CFT Law recognises **5 types of TCSP activities**:

- **Incorporation**: Forming companies or other legal persons;
- **Directorship and secretarial services**: Acting as or arranging for another person to act as a director, manager, member of the board of directors, member of the executive board or secretary of a company, a partner of a partnership, or a similar position in relation to other types of legal persons;
- **Domiciliation**: Providing a registered office, business address, correspondence or administrative address or business premises and, where applicable, other related services for a company, a partnership or any other legal person or arrangement;

- **Fiducie/trust**: Acting as, or arranging for another person to act as, a fiduciaire in a fiducie (as defined the 2003 Fiducies and Trust Law), a trustee of an express trust or an equivalent function in a similar legal arrangement; and

- **Nominee shareholder**: Acting as, or arranging for another person to act as, a nominee shareholder for another person.

TCSPs may be exposed for multiple reasons

- The **sector is large and diverse**, with a variety of licensed professionals and activities that can be conducted. Detection of ML threats may prove challenging in a market where diverse TCSPs and products exist.
- The **international nature of the business**, foreign client base and foreign ownership of assets, may increase the likelihood of dealing with illicit proceeds.
- **Challenges in UBO identification and origin of funds/wealth** as a result of the diverse nature of clients which includes legal entities and arrangements in the shareholding structure which may enable the beneficial owner to hide his identity, particularly in instances where the primary relationship is with an intermediary advising the client.

- **Intermediation of the relationships** between a TCSP and client because of the presence of intermediaries (e.g. lawyers, accountants, business providers, advisors). This can reduce transparency around client identity.
- **Services** offered by TCSPs may be abused or misused to conceal the identity of the beneficial owner or their source of funds and facilitate the laundering of illegal proceed.

Threats for Specialised PFS

- **Specific Money Laundering threats**

There are three specific predicate offences that are most relevant for Specialised PFS performing TCSP activities, which are: fraud and forgery, tax crimes, corruption and bribery

- **Terrorism Financing threats**

There has been a significant change in how terrorists and terrorist organisations finance their operations. While they initially relied heavily on donations from sympathizers, they now increasingly turn to illegal activities as their primary sources of funding. These activities include extortion, drug trafficking, and kidnapping, which are primary offences of money laundering.

Profileration Financing threats

The primary driver of these risks for Specialised PFS providing corporate services is that these services are deemed high risk in international guidance given they could be misused to obfuscate links between transactions and designated persons/entities. The United Nations Security Council indicated that designated persons and entities, and those persons and entities acting on their behalf have quickly adapted to financial restrictive measures and developed complex schemes to make it difficult to detect their illicit activities.

Risk mitigation (sample)

- **Identify, assess and understand the ML/TF risks**. The risk assessment should then drive the application of the professional's risk-based approach to AML/CFT.
- Specialised PFS have defined a ML/TF **risk appetite**.
- Specialised PFS are also required to apply **control measures in relation to customer due diligence (CDD)** at on-boarding and throughout the life of the business relationship.
- Where ML/TF risks are higher, an **enhanced due diligence** (EDD) will need to be performed.

- Specialised PFS have a **client acceptance policy** based on a risk-based approach and different levels of internal authorisation in place.
- Specialised PFS are required to conduct ongoing due diligence on the business relationship and **transaction monitoring.**
- Specialised PFS have in place **ongoing employee training** and awareness-raising programmes to ensure staff understand ML/TF risks and AML/CFT obligations
- **Strong leadership** and engagement by senior management and the board of directors in AML/CFT is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance, ensuring that staff adheres to the firm's policies, procedures and processes designed to limit and control risks

Risk mitigation measures taken by the CSSF

- **CSSF promotes an understanding of ML/TF risks and AML/CFT** obligations through multiple channels.
- CSSF also performs a **risk assessment on all Specialised PFS**. This includes a risk assessment on the basis of findings by internal and external control functions, existence of policies, controls and procedures, provision of ongoing employee training and awareness-raising programmes to ensure staff understand ML/TF risks, AML/CFT obligations and the obligation to cooperate with authorities.
- CSSF operates AML/CFT **market entry controls** at the instruction of a Specialised PFS, (including a licensing process) and at any subsequent change within the ownership structure.

- **Fit and proper checks** are carried out on the management and ownership structure of the Specialised PFS in instruction and during the lifetime of the Specialised PFS.
- **Ongoing desk-based review** of AML/CFT relevant information and documentation (such as review of the closing documents of the Specialised PFS…).
- **Regular interactions with the professional**, including face-to-face meetings and/or calls performed on a risk basis.
- **Annual AML/CFT questionnaire** with specific questions depending on the activities of the Specialised PFS to collect additional information.

- 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.
- The CSSF has significantly **increased its staff** number both in the Specialised PFS off-site department and in the on-site department.
- Both the offsite and onsite inspection divisions can trigger **remediation and enforcement** and have at their disposal a wide range of supervisory tools. Enforcement follows the "Procédure Administrative Non-Contentieuse (PANC)" process.

Most frequent off- and on-site findings (best practices)

- Establishing a clear **AML/CFT risk appetite** statement and communicating it throughout the organization.
- Promoting a **strict compliance culture** throughout the organisation, especially in the first line of defence.
- Performing **Targeted Financial Sanctions, PEP and adverse media screening** to ensure screening is done immediately after an update in the sanction lists.
- Performing **transaction monitoring**.
- **Complete documentation/information** on the origin of funds, source of wealth, the identity of legal persons and beneficial owners.

CSSF recommendations to the private sector (sample)

- Specialised PFS should 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** and develop proportionate and effective controls.
- Take appropriate steps to **identify and assess firm-wide ML/TF risks**.
- **Implement a clear AML/CFT risk appetite** and strategy.
- Ensure that name screening against **Targeted Financial Sanctions screening** is performed immediately as required notably by EU regulations.

- **Review client relationships on a periodic basis** to determine whether ML/TF risk has changed.
- Ensure that the **transaction monitoring process is effective** and adapted to the activity performed and the type of client.

- **Report without delay suspicious activities and transactions** to the CRF and targeted financial sanction breaches to the Ministry of Finance.
- Ensure that **resources dedicated to AML/CFT are commensurate with the professional's level of risk**.

- The CSSF expects SPFS **to reflect the findings and conclusions from this SSRA into their frameworks** to ensure they remain appropriate to effectively mitigate ML/FT risks.

Thematic review on terrorist financing ("TF")

Outcome of the Thematic review carried out in 2025

cssf
Commission de Surveillance
du Secteur Financier

Context

2023 FATF mutual evaluation report (recommendation for immediate outcome 1):

"Luxembourg should further develop its understanding of TF risks and vulnerabilities stemming from its role as international financial centre, and transit jurisdiction for foreign TF financial flows and businesses linked to TF activity, including undertaking a qualitative assessment of what Luxembourg legal persons are used for, their links to higher-risk jurisdictions and other intelligence and investigatory materials from law enforcement and other authorities."

cssf

TF risks - Reminders

Result of the 2022 Terrorist Financing Vertical Risk Assessment ("TF VRA"):

- None of the sub sectors in which PSF SP are active have been considered as vulnerable to TF.
- POST (not a PSF SP but supervised by our department): please refer to retail banks (high inherent risk and medium residual risk).
- Mortgage credit intermediaries (not a PSF SP but supervised by our department): not in scope of the TF VRA.

Scope

- Trust and Company Service Providers (« TCSP »): to include it in the Sub Sector Risk Assessment of PSF SP providing corporate services but some conclusions can be of use to all professionals.
- TF risk self-assessments (14 interviews).
- Clients held by Non Profit Organisations (« NPOs ») (4 TCSPs).
- Beneficial Owners (« BO») in Israel and the United Arab Emirates (UAE) (9 TCSPs).

cssf

CSSF conclusions on the TF Risk self-assessments of TCSPs

- TF risks not always covered (no explanations, rating) or limited explanations (2 sentences).
- TF risks mixed with ML risks.
- TF risks were often **overestimated** (very cautious, not tailor made, focus on reputation).

Legal References to remember:

- Article 2-2 (1) of the Law on the fight against money laundering and terrorist financing("AML/CFT Law") states that *"the professionals shall take appropriate steps to **identify, assess and understand** the risks of (…) terrorist financing that they face".*
- Article 2-2 (2) of the AML Law: *"the professionals shall consider **all relevant** risk factors before determining the overall risk level".*

cssf

TF Risk self assessment – example of issues detected number 1

- « *The evaluation of the PFS's vulnerability to Terrorist Financing (TF) risk is not treated as an independent element within its Risk-Based Approach (RBA). Instead,* ***it is included in the ML/TF risk scoring****.* »

Comments CSSF:

- No separate TF analysis and risk rating to be reported in the Questionnaire on Financial Crime.
- FATF (*terrorist financing risk assessment guidance)*:
  « Crucially the factors associated with TF risk are also distinct from those associated with ML risk. (…) Although there may be some overlap in the potential vulnerabilities that criminals and terrorists misuse, the motive, and therefore the threat and risk indicators, differs ».

cssf

TF Risk self assessment – example of issues detected number 2

Client risks:

- *"Presence of non-profit organizations and then states, individuals, or corporate groups with potential interests in financing terrorism;*
- *Clients involved in cash-intensive sectors;*
- *High number of suspicious activity reports filed for TF."*

Comments CSSF:

- Theoritical risk factors quoted to explain a high risk rating but in fact none of them were applicable to the TCSP.

TF Risk self assessment – example of issues detected number 3

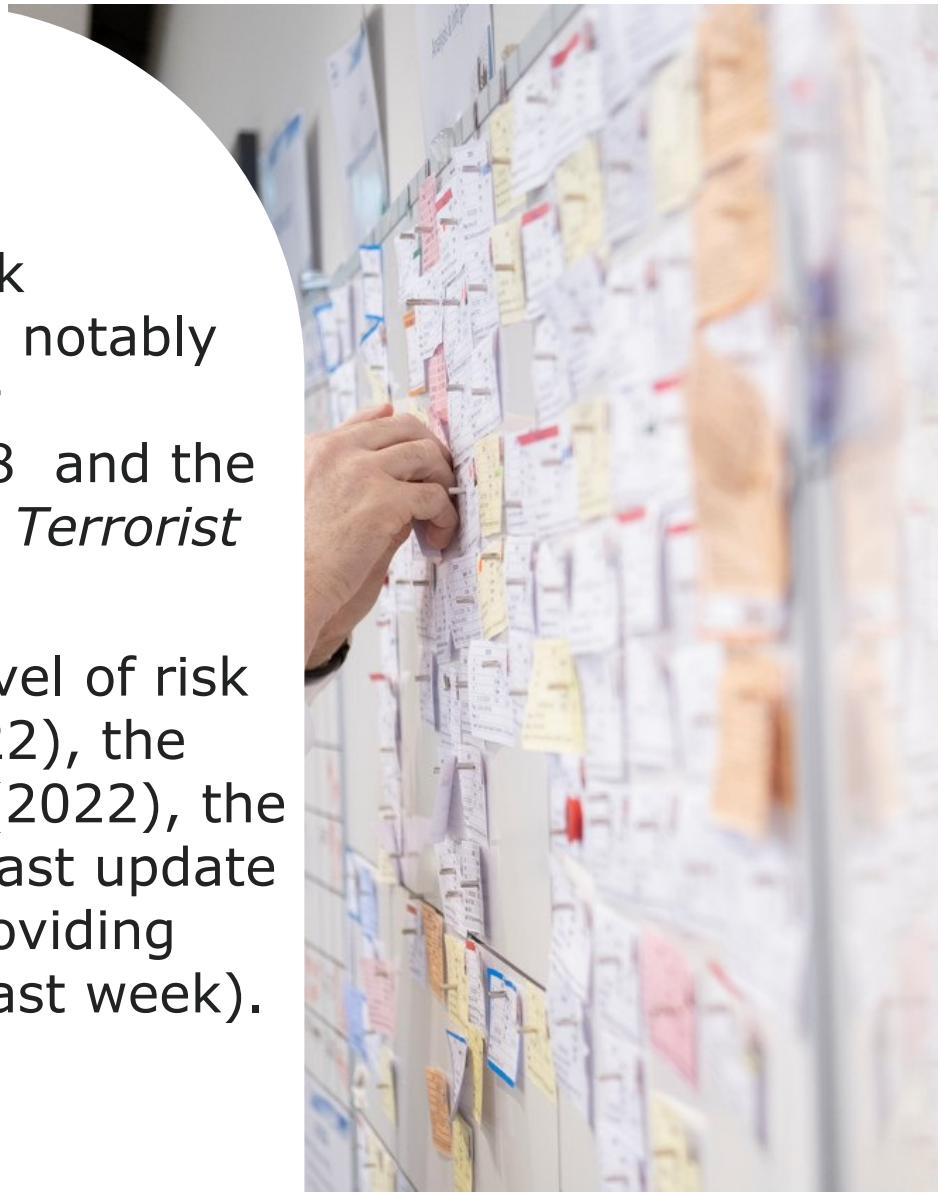
- *"Considering the regulatory guidance, **including NRA 2025**, prior assessments, and market trends, the PFS is formalizing the Risk Assessment 2025 reclassifying TF risk from high to medium."*

Comments CSSF:

- The 2025 ML National Risk assessment (« NRA ») does not cover TF.

Useful references for your TF risk self assessment

- Relevant legal references explaining risk assessments and risk indicators include notably CSSF circular 11/529 and CSSF circular complemented by Circular CSSF 25/878 and the FATF report "*Comprehensive update on Terrorist Financing risks*").
- Other relevant sources to assess the level of risk include (as applicable) the VRA TF (2022), the VRA legal persons legal arrangements (2022), the SSRA on collective investment sector (last update 2025), the SSRA on Specialised PFS providing TCSP services if applicable (published last week).



CSSF conclusions on clients held by NPOs and BOs in Israel and UAE

- No TF deficiencies found showing that the mitigation measures applied to ML are also effective for TF.
- Limited presence of NPOs in clients structures and UBOs linked to TF countries (Israel and UAE mostly represented) and no links to terrorists/terrorist groups/financing of TF needs (propaganda…).

cssf

Points of attention to consider for the future:

- Legal persons (not just NPOs) are also abused for TF "*Terrorist groups, such as Hamas, and other illicit actors use increasingly sophisticated money laundering techniques including smuggling cash and using **shell companies** to avoid detection and hide their involvement in financial transactions.*"
- Possible links between TF and organised crime *"As methods based on front and shell companies are already widely spread in the field of ML, any further convergence between organised crime and TF could result in such schemes becoming more common"*

- Sources:
- How Hamas raises, uses, and moves money - Atlantic Council
- FATF Comprehensive update on terrorist financing risks

cssf

Final conclusions and best practices in relation to TF

SSRA of PSF SP providing corporate services (TCSP services) (residual risk) (2026):

"The CSSF considers the risk to be very low"

Understanding of TF risks has already improved among PSF SP as a result of this thematic review. **Guidance/Good practices:**

- Separate TF risk assessment.
- Specific TF training including case studies, TF red flags.
- Transaction monitoring: Checks in the transaction messages: suspicious communications?
- Transaction monitoring: Checks countries involved (all parties including financial institutions).
- Name screening: update of lists (automated tools) and checks without delay.

cssf

Thank you

cssf
Commission de Surveillance
du Secteur Financier

LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier
(CRF)

Specialised PFS: CRF updates

Luxembourg, January 26th 2026

Agenda

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

- Key figures for 2025
- Reflecting on reporting & Key Data re. specialised PFS
- Key figures and insights on terrorist financing
- Compliance corner: New Feedback Template for Reporting Entities & Sector specifics
- Financial Restrictive Measures (Russia)
- Emerging typologies (AI Deepfakes & BEC Fraud)

LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier (CRF)

1 – Key Figures for 2025

FIU Luxembourg (CRF)

2025 key figures (The numbers presented are indicative only and shall not be construed as final)

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

~ 68 000
Filed reports

~ 15 000
Registered professionals on goAML

1 995
Disseminations sent by Luxembourg FIU

In addition, cross-border reporting is done via FIU.net

1 133
Disseminations received from foreign FIUs

~ EUR 162 mio
of assets frozen in 2024

100%
Digital and paperless

Top 5
Associated Predicate Offences

- Fraud
- Counterfeiting and product piracy
- Tax offences
- Money laundering

Top 5
International cooperation - Information to foreign countries

Top 5
International cooperation - Information from abroad

~ 600
Financial analysis reports submitted to judicial authorities and other national AML/CFT authorities

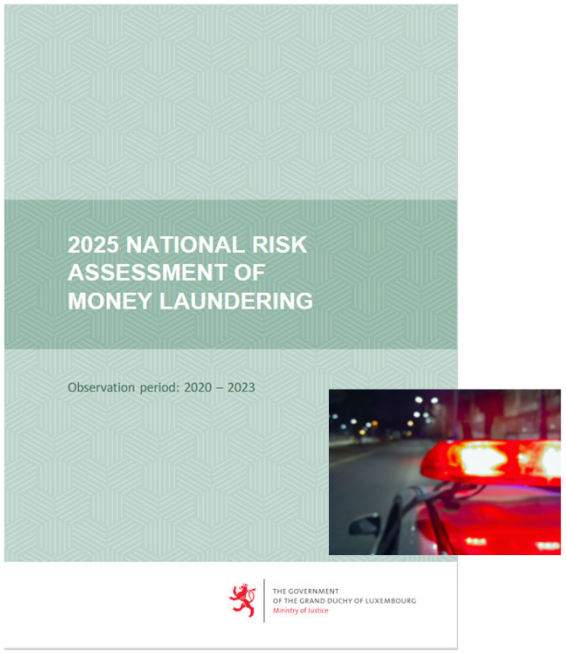
LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier
(CRF)

2 – Specialised PFS: Reflecting on reporting & Key data for 2025

Luxembourg's NRA : Specialised PFS - ML/TF risk exposure

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)



NRA: High Inherent ML risk for specialised PFS providing Corporate services though!

Sector	Sub-sector	2025 NRA: Inherent risk	2025 NRA: Residual risk
Specialised PFSs	Professional depositaries	Medium	Low
Support PFSs and other specialised PFSs[393]	Support PFSs	Very Low	Very Low
	Other specialised PFSs		
Legal persons and legal arrangements	*Sociétés commerciales*	Very High	Medium
	Sociétés civiles	Medium	Low
	NPOs (as per FATF definition) carrying out primarily international activities – ASBLs and *Fondations*[395]	High	High
	NPOs (as per FATF definition) carrying out local activities – ASBLs[396]	Low	Low
	NPOs (as per FATF definition) carrying out local activities – *Fondations*[397]	Low	Very Low
	Other legal persons	High	Medium

BUT

Bearing in mind!

Link here!

Do not mix the RBA with Suspicions!

Inherent Risk → *Mitigation* → Residual Risk

Will the reporting evolve ?
Prioritization, Relevance and Quality: Art. 69 (2) of the new (EU) AML Regulation

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

- Art. 69 (2) AMLR: "*For the purposes of paragraph 1, obliged entities shall assess transactions or activities carried out by their customers on the basis of and* ***against any relevant fact and information*** *known to them or which they are in possession of. Where necessary, obliged entities* ***shall prioritise their assessment*** *taking into consideration the urgency of the transaction or activity and the risks affecting the Member State in which they are established*".

✓ Assessment to be based on relevant facts & information

✓ Prioritization where necessary

"*A suspicion pursuant to paragraph 1, point (a), shall be based on the* ***characteristics of the customer and their counterparts****, the* ***size and nature of the transaction or activity*** *or* ***the methods and patterns*** *thereof, the* ***link between several transactions*** *or activities,* ***the origin, destination or use of funds****, or any other circumstance known to the obliged entity, including* ***the consistency of the transaction or activity*** *with the information obtained pursuant to Chapter III including the risk profile of the client*".

✓ **NEW: Efficiency** in the reporting
(Currently no such level of details in Art. 5 of the AML Law)

Quality of reportings in the FATF MER (2023)

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

FATF IO 6 conclusion pinpointed issues re. the "*relevancy and accuracy of information received from obliged entities (…) impacting the quality of the CRF work and responsiveness*"

→ "ADEQUATE, ACURATE & UP TO DATE INFO"

FATF IO 4 emphasized that "*a large proportion of reports are driven by adverse media hits which not all FIs (…) properly analyse to establish if there are grounds for suspicion before filing the report*"

→ *THE **NEW CRITERIA SET IN ART. 69 (2) AMLR** WILL COME HANDY HERE !*

Reporting "promptly" (STRs/SARs)

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

AML Law of 12 November 2004

- **Art. 5, 1 (a) AML Law:** "*(…) the professionals (…) are required to: (a) inform **promptly** ("sans délai"), on their own initiative, the Financial Intelligence Unit (…) when they know, suspect or have reasonable grounds to suspect that money laundering, an associated predicate offence or terrorist financing is being committed or has been committed or attempted, (…)*"

QUID with the new (EU) AMLR ?

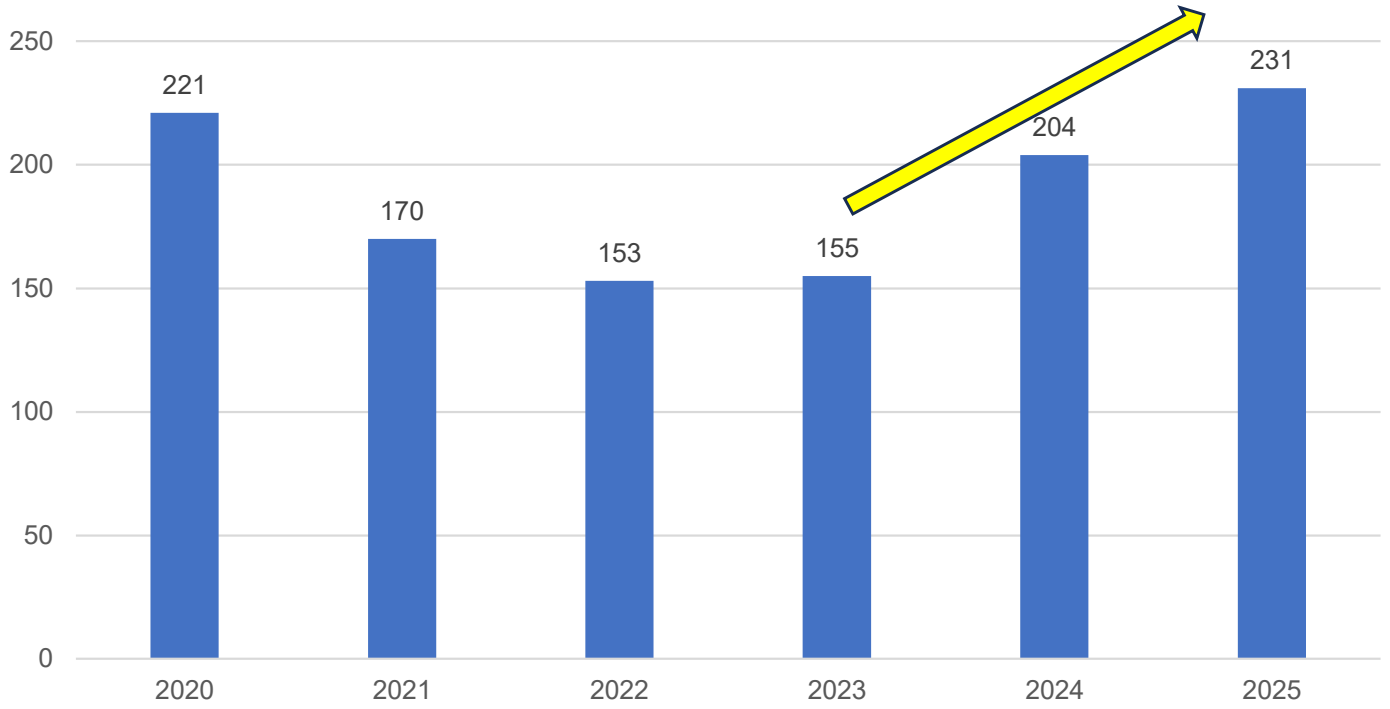
- Recital 140 (AMLR): "*FIUs should be able to obtain **swiftly** from any obliged entity all the necessary information relating to their functions" (…)*
- Art.69 (1) (AMLR): "*Obliged entities, and, where applicable, their directors and employees, shall cooperate fully with the FIU **by promptly**: (a) **reporting** to the FIU (…)*"

✓ No changes here:
STRs/SARs shall be reported "promptly"!

Mind the delays in case of a National Request of Information !

SARs/STRs filed by specialised PFS
(2020 – 2025)

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

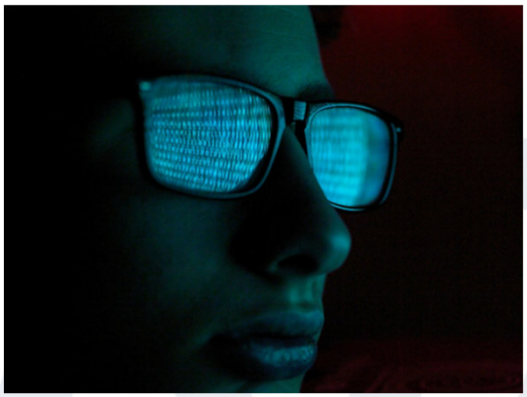


Your reporting in light of NRA 2025

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

Table 7: Threats assessment, weighted average exposure

Predicate offence	External threat level (75%)	Domestic threat level (25%)	Weighted average exposure
Fraud and forgery	Very High	High	Very High
Tax crimes	Very High	Medium	Very High
Corruption and bribery	Very High	Medium	Very High
Drug trafficking	High	High	High
Participation in an organised criminal group and racketeering	High	Medium	High
Sexual exploitation, including sexual exploitation of children	High	Medium	High
Cybercrime	High	Medium	High
Counterfeiting and piracy of products	High	Low	High



- Make sure that your suspicions match the predicate offences highlighted in the NRA !

- Do adapt your procedures according to the findings of the NRA and the newly released CSSF SSRA

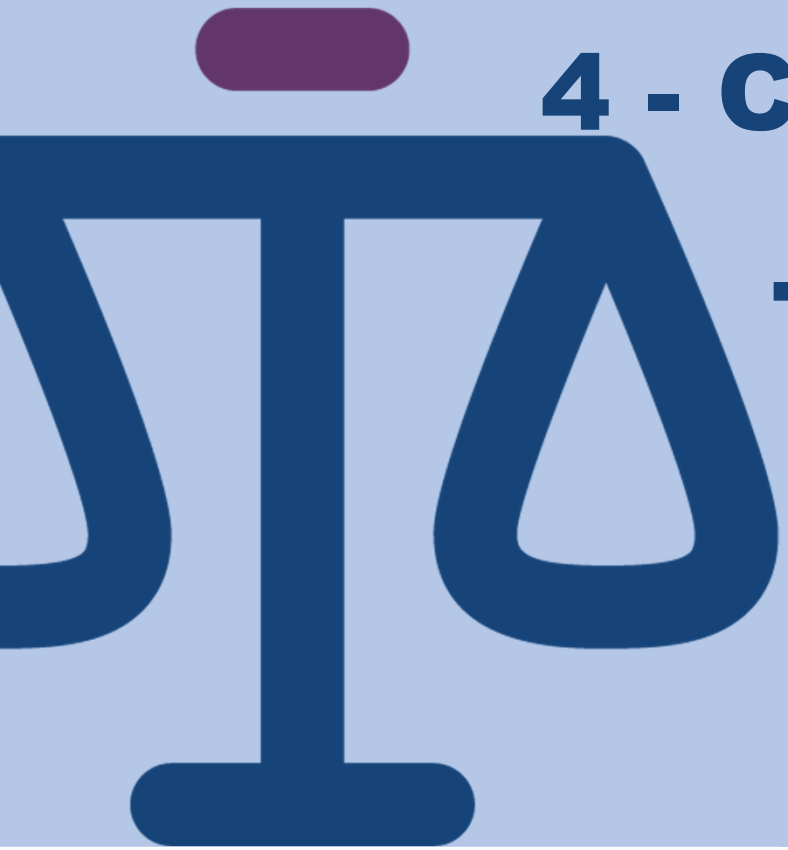
LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier
(CRF)

3 - KEY FIGURES AND INSIGHTS ON TERRORIST FINANCING

LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier
(CRF)



4 - COMPLIANCE CORNER: NEW FEEDBACK TEMPLATE FOR RES & SECTOR SPECIFICS

Future content of the new Feedback template for REs

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

General overview

Evolution of STRs/SARs
Evolution of TFTRs/ TFARs
(latest 9 TRIM)

Follow-up I

Information received when File is closed

Follow-up II

Exchange of Info with foreign counterparts

Report Quality Feedback

.

LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier
(CRF)

5 – FINANCIAL RESTRICTIVE MEASURES (RUSSIA)

Current Legal Framework (Luxembourg)

LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier (CRF)

Law of 19 December 2020 on the Implementation of Financial Restrictive Measures (FRM):

(i) Implementing automatically the FRM adopted by United Nations' Security Council and

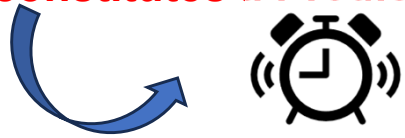
(ii) Various Acts of the European Union: Common positions, Decisions and Regulations (of direct application)

Art. 10: **Failure to comply** with the RM "*adopted by way of and Act by the European Union*"

Law of 20 July 2022 setting up a monitoring committee for restrictive measures in financial matters:

(i) Setting-up a committee to "monitor" the implementation of financial sanctions

(ii) Amending Art. 506-1 of the Criminal Code **= a Breach of Art. 10 of the Law on FRM constitutes a Predicate Offence of Money Laundering !**



Triggers the competence of the CRF !

EU Regulations focusing on Russia

LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier (CRF)

- Council Regulation (EU) N°833/2014 of 31 July 2014 *concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine: ("MEASURES")*
  - More focused on financial instruments/bank accounts issued/held by persons of Russian nationality or residing in Russia, the Russian state, Russian financial institutions/companies and other FRM.
- Council Regulation (EU) N°269/2014 of 17 March 2014 *concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine: ("PERSONS")*
  - Mostly targets directly specific persons and imposes a freeze on their assets/economic resources.

Violations of specific provisions of these two Regulations will fall within the remit of Art. 10 of the FRM Law !

Overall core Typologies

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

Undervalued shares transfers

- Use of non-sanctioned persons to acquire Luxembourg and EU-based companies on behalf of a sanctioned person via share transfers at a suspiciously low share price.

Straw investment channels

- Indirect investments made in investment funds by offshore front companies or straw men on behalf of underlying sanctioned UBOs.

Legal proxy shield

- Use of foreign law firms to conduct transactions on behalf of sanctioned individuals.

Breach of export bans

- Use of commercial companies suspected of exporting goods to Russia via neighboring and/or facilitating countries in the context of corporate and correspondent banking relationships.

Third-party (re)payments

- Loan repayments or invoice payments performed by a non-sanctioned third-party individual or entity on behalf of a sanctioned individual.

Use of professional enablers/facilitators

- Use of professional enablers/facilitators to set up sanction evasion schemes.

LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier
(CRF)

6 - EMERGING TYPOLOGIES

Trend alert 1 - Use of Deepfakes/AIs

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

- ✓ Personal EMoney **fraudulent accounts opened remotely** & used as **mule accounts**
- ✓ Use of **pre-recorded video (using AI), also with the use of fake ID documents** (unfortunately not detected @ onboarding stage)
- ✓ Fraudulent account being credited by third parties with no apparent link with the fraudster account (scam occurs here)
- ✓ Funds then promptly transferred to third parties foreign accounts (online transfers **or** payment cards using crypto currency exchange platform)

Trend alert 2 - Business Email Compromise targeting the investment Sector

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

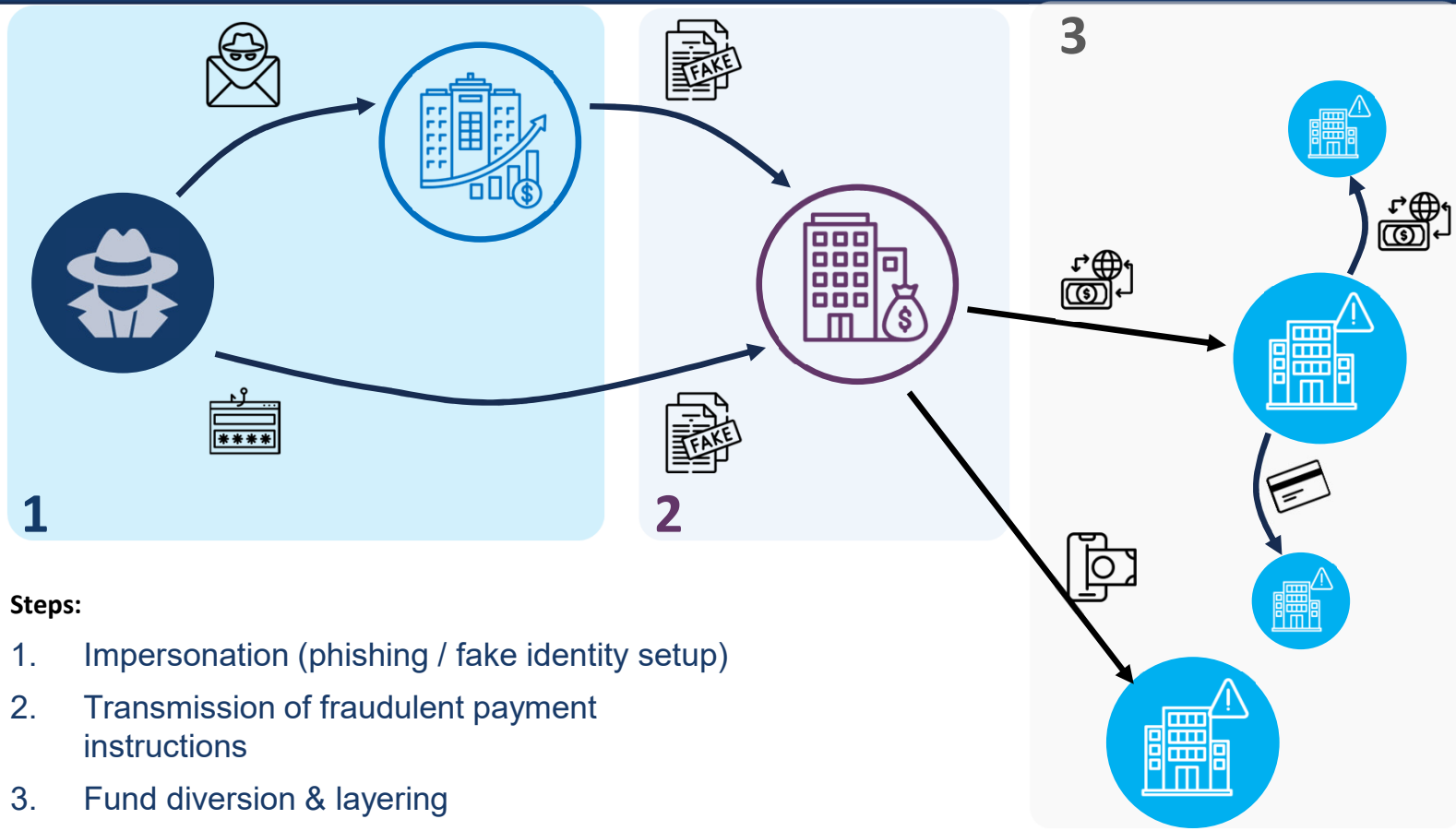
- ✓ Increasing number of SARs involving cyber enabled fraud schemes targeting the investment sector
- ✓ Scams using fake capital calls or drawdown notices, usually involving **Business Email Compromise** and other impersonation techniques
- ✓ High value transactions
- ✓ FUND MANAGERS, ADMINISTRATORS, INVESTORS, **TCSPs**

<u>Make sure that you do have robust procedures to deter such frauds</u>:

→ ✓ *Art. 4, para (1), a) of the AML Law of 2004 (Adequate Internal Management Requirements)*

BEC Fraud:
How does it look like ?

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)



Steps:

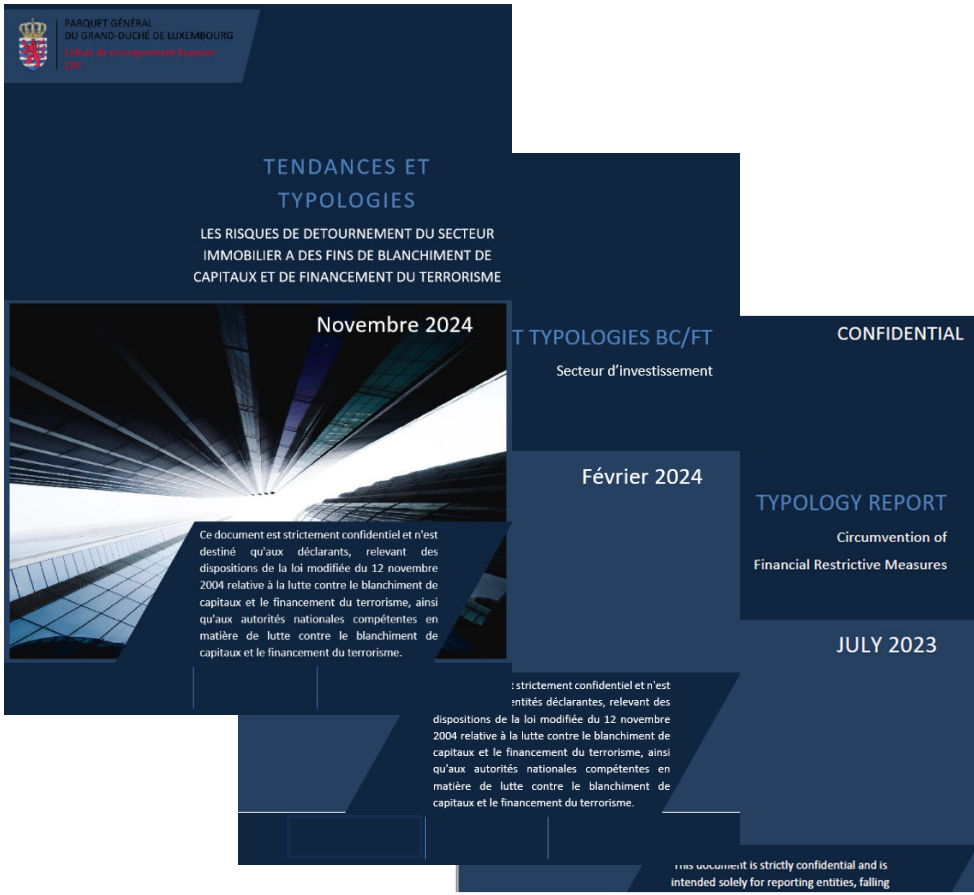
1. Impersonation (phishing / fake identity setup)
2. Transmission of fraudulent payment instructions
3. Fund diversion & layering

Publications and typology reports from Luxembourg FIU (CRF)

LA JUSTICE
Grand-Duché de Luxembourg
Cellule de Renseignement Financier (CRF)

Luxembourg FIU (CRF) regularly releases sector-specific and general trends and typologies reports.

Latest trend alerts on: (i) Deepfakes & AI to circumvent AML preventive measures and (ii) BEC targeting the IS.



LA JUSTICE
Grand-Duché de Luxembourg

Cellule de Renseignement Financier
(CRF)

Thank you for your attention!

National Risk Assessment
Money Laundering

Observation period: 2020 - 2023

26/01/2026

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Justice

Contents

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- **Part I:** The central role of the NRA in the AML/CFT framework and the risk-based approach
- **Part II:** The NRA ML – main findings and conclusions of the 2025 update

Part I

The central role of the NRA in the AML/CFT framework and the risk-based approach

FATF Recommendation 1 – Assessing risks and applying a risk-based approach and its Interpretative note obligations and decisions for countries

- **Identify, assess and understand** ML/TF risks for the country
- Designate an authority or mechanism to **coordinate** actions to assess risks, and apply resources, aimed at ensuring that risks are effectively mitigated → *Steering Committee; Prevention Committee*
- Apply a **RBA** to ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified (= essential foundation to efficient allocation of resources across the AML/CFT regime)
- Keep the assessments up-to-date and have mechanisms to provide appropriate information on the **results** to all relevant stakeholders
- Where countries identify **higher risks**, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify **lower risks**, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions (in line with the NRA)

Countries should require obliged entities and professionals to identify, assess and take effective action to mitigate their risks

Practical implications for the private sector

Interpretative note to FATF R1 concerning obligations to professionals

Assessing ML/TF risks

Professionals should be required to take appropriate steps to identify and assess their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels) → *Link to the NRA methodology*

- These assessments should be appropriate to the **nature** and **size** of the business

Risk management and mitigation

- Professionals should be required to have **policies, controls and procedures** that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the professional)
- Where **higher risks** are identified, professionals should be required to take enhanced measures to manage and mitigate the risks
- Where **lower risks** are identified, countries may allow professionals to take simplified measures to manage and mitigate those risks
- The measures taken to manage and mitigate the risks (whether higher or lower) should be **consistent** with national requirements and with guidance from competent authorities and SRBs

Different levels of granularity of risk assessments

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Macro analysis

- At EU or national level
- Focus of the supra-national risk assessment (EU) and the NRA (Luxembourg), with macroeconomic and financial data, criminality rates, demographics…
- Aims to identify, assess and understand ML/TF risks at the EU/national level
- Allows elaborating a global strategy (EU or Luxembourg) and prioritising of resources across agencies

Micro analysis

- At product/activity/crime/techniques, entity level
- Focus of entity-level risk assessments with granular data about products, typologies, case studies, types of entities…
- Aims to identify, assess and understand ML/TF risks at the product/activity level
- Allows applying specific rules to products/activities following their risk level and for instance guide supervisors when conducting controls (e.g.: prioritisation of target entities, products, etc)

Meso (or intermediate) analysis:

- At the (sub-)sector level (e.g.: Legal persons and legal arrangements vertical risk assessment at the national level; Private banking; collective investments by the CSSF)
- Focus of (sub-)sector risk assessments with aggregated micro data, surveys, questionnaires…
- Aims to identify, assess and understand ML/TF risks at the (sub-)sector level
- Allows understanding risks at the (sub-)sector level and elaborating a specific (sub-)sector strategy

Part II

The NRA ML – main findings and conclusions of the 2025 update

NRA – overall approach

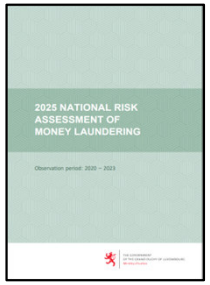
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Fight against ML and TF	ML and TF
➢ Common legal framework ➢ May exploit the same vulnerabilities of a product or service	➢ Own specificalities ➢ Differ in their nature, source and purpose

A separate analysis:

- allows for a **better understanding** of the particular drivers of each type of risks
- facilitates the implementation of more targeted and ultimately **more effective mitigation actions**

Two separate risk assessments:



NRA – overall approach

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Luxembourg NRA Step 1: Inherent risk assessment (i.e. in the absence of mitigating factors)

Threats
The objective of the threats analysis is to understand the environment in which predicate offences are committed to identify their nature and to assess the exposure to them

→cf. slides: 10 - 16

Vulnerabilities
The aim of the vulnerability analysis is to determine the exposure of each sub-sector subject to AML/CFT obligations to money laundering risks

Inherent risk
Inherent risk reflects the level of risk without taking into account mitigating factors (e.g. private sector controls, supervisors, etc.). This risk level can be considered as the "gross" level of risk

→cf. slides: 17 - 22

Luxembourg NRA Step 2: Mitigating factors and residual risk

Inherent risk

-

Mitigating factors
The aim of the mitigating factor analysis is to assesses the effectiveness of mitigating measures that are in place (e.g. legislation, private sector controls, supervisors' actions, etc.)

→cf. slides: 23 - 25

=

Residual risk
Residual risk reflects the level of risk once mitigation measures are applied. This risk level can be considered as the "net" level of risk

→cf. slides: 26 - 30

Threats assessment

National ML risk assessment 2025

Threats scorecard

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

This scorecard is used to assess the probability, proceeds and consequences of each crime category assessed in the context of the NRA exercise

Criteria	Sub-criteria	Example of indicators that can be used
Probability of crime ("likelihood")	Level of criminality	Crime rate/number of crimes (domestic) Terrorist events (incidents, attempts, casualties, etc.) Presence and activities of known terrorist groups Number of offences, open/new notices, prosecutions and convictions (with and without ML)
Proceeds of crime ("size" and "complexity")	Proceeds generated	Amounts seized Estimated value generated per crime committed Estimate of trade and financial flows with foreign countries (in particular with high risk countries) Estimated value of proceeds from international crimes Number of STRs and SARs filed
	Form of proceeds	Cash proceeds vs. Non-cash physical Use of innovative forms (e.g. virtual currencies)
	ML expertise	Sophistication (knowledge, skills, expertise) Capability (network, resources, etc.)
	Geography	Origin/source Destination
Human, social and reputational impact ("consequences")	Economic and social cost	Foregone revenues Financial system stability and its perceived integrity Attractiveness of the country for business, ability to attract FDI, broad "reputation" of country

National exposure to ML threats

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Considering Luxembourg's important financial centre, the **external threat** level reflects the **threat that proceeds from crimes committed abroad are laundered via Luxembourg**

The domestic exposure to ML is significantly smaller (low crime) and reflects the threat that **crimes are committed in Luxembourg** and related proceeds are laundered in the country or abroad

Predicate offence	External threat level (75%)	Domestic threat level (25%)	Weighted average exposure
Fraud and forgery	Very High	High	Very High
Tax crimes	Very High	Medium	Very High
Corruption and bribery	Very High	Medium	Very High
Drug trafficking	High	High	High
Participation in an organised criminal group and racketeering	High	Medium	High
Sexual exploitation, including sexual exploitation of children	High	Medium	High
Cybercrime	High	Medium	High
Counterfeiting and piracy of products	High	Low	High
Smuggling	Medium	Low	Medium
Insider trading and market manipulation	Medium	Low	Medium
Robbery and theft	Medium	High	Medium
Trafficking in human beings and migrant smuggling	Medium	Medium	Medium
Illicit trafficking in stolen and other goods	Medium	Low	Medium
Extortion	Low	Low	Low
Illicit arms trafficking	Low	Low	Low
Environmental crime	Low	Low	Low
Murder and grievous bodily injury	Low	Low	Low
Kidnapping, illegal restraint and hostage taking	Low	Low	Low
Counterfeiting currency	Low	Very Low	Very Low
Piracy	Low	Very Low	Very Low

Threats assessment

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Remarks:

- Availability and granularity of data per crime varies
- Important number of stakeholders involved (located at different points within the enforcement and penal chain)

→Threat level = combination of quantitative and qualitative information

→Flexibility between different categories: one offence can be linked to another

External exposure: focus on top three threats

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Predicate offence	External threat level (75%)	Domestic threat level (25%)	Weighted average exposure
Fraud and forgery	Very High	High	Very High
Tax crimes	Very High	Medium	Very High
Corruption and bribery	Very High	Medium	Very High
Drug trafficking	High	High	High
Participation in an organised criminal group and racketeering	High	Medium	High
Sexual exploitation, including sexual exploitation of children	High	Medium	High
Cybercrime	High	Medium	High
Counterfeiting and piracy of products	High	Low	High
Smuggling	Medium	Low	Medium
Insider trading and market manipulation	Medium	Low	Medium
Robbery and theft	Medium	High	Medium
Trafficking in human beings and migrant smuggling	Medium	Medium	Medium
Illicit trafficking in stolen and other goods	Medium	Low	Medium
Extortion	Low	Low	Low
Illicit arms trafficking	Low	Low	Low
Environmental crime	Low	Low	Low
Murder and grievous bodily injury	Low	Low	Low
Kidnapping, illegal restraint and hostage taking	Low	Low	Low
Counterfeiting currency	Low	Very Low	Very Low
Piracy	Low	Very Low	Very Low

External exposure: focus on top three threats

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

➢ Fraud and forgery

- Cyber-enabled fraud (FATF, Egmont Group, Interpol): on the rise (new technologies, digitalisation); proceeds tend to be laundered through a network of accounts (involving individual money mules, shell companies controlled by criminals, legitimate business)
- Fraud affecting the EU's financial interests (expenditure fraud): overall increasing amount of EU spending (especially post Covid-19)

→Luxembourg's position as a payments, investment and cyber hub increases the likelihood that criminals potentially launder the proceeds of fraud via Luxembourg

➢ Tax crimes

- Globally, legal persons and arrangements are observed to be misused for tax crimes (direct and indirect taxes)
- Some level of knowledge/sophistication required to commit tax crimes
- VAT fraud: exposure through payment hub processing transactions in relation with e-commerce (fraudulent businesses trying to evade VAT obligations) and Luxembourg legal persons (conduit companies in VAT carousel fraud, MTIC fraud)

➢ Corruption and bribery

- Luxembourg context: (1) limited size of domestic market: Luxembourg's economy is internationally oriented; (2) Luxembourg's financial centre is a preferred destination for investment and corporate group activities
- Considering the level of expertise required and the high level of proceeds involved, sophisticated sectors are probably more likely to be targeted by criminals
- Cost of corruption estimated to be significant (6% of EU's GDP)

Domestic exposure: focus on top three threats

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Fraud and forgery generate, together with drug trafficking, the most important proceeds in Luxembourg

Theft ("vols simples") is the most reported criminal offence registered with the Police

Predicate offence	External threat level (75%)	Domestic threat level (25%)	Weighted average exposure
Fraud and forgery	Very High	High	Very High
Tax crimes	Very High	Medium	Very High
Corruption and bribery	Very High	Medium	Very High
Drug trafficking	High	High	High
Participation in an organised criminal group and racketeering	High	Medium	High
Sexual exploitation, including sexual exploitation of children	High	Medium	High
Cybercrime	High	Medium	High
Counterfeiting and piracy of products	High	Low	High
Smuggling	Medium	Low	Medium
Insider trading and market manipulation	Medium	Low	Medium
Robbery and theft	Medium	High	Medium
Trafficking in human beings and migrant smuggling	Medium	Medium	Medium
Illicit trafficking in stolen and other goods	Medium	Low	Medium
Extortion	Low	Low	Low
Illicit arms trafficking	Low	Low	Low
Environmental crime	Low	Low	Low
Murder and grievous bodily injury	Low	Low	Low
Kidnapping, illegal restraint and hostage taking	Low	Low	Low
Counterfeiting currency	Low	Very Low	Very Low
Piracy	Low	Very Low	Very Low

Vulnerability assessment

National ML risk assessment 2025

Vulnerability scorecard

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

This scorecard is used to assess the inherent risk level of each sub-sector analysed in the context of the NRA exercise

Dimension	Sub-dimension	Examples of indicators/data needed
Structure	Size	• Revenue/turnover and profit • Assets • Assets under management
	Fragmentation/complexity	• Number of institutions • Level of concentration (e.g. top 5 entity assets as a % of the market)
Ownership/ legal structure	Ownership/ legal structure	• % ownership by foreign beneficial owners (of which from risky countries based on FATF lists) • % of entities with foreign mother
Products/activities	Products/activities	• % of high risk products (e.g. % revenue from products/activities)
Geography	International business	• % of international business (e.g. in clients revenue, assets, transactions)
	Flows with weak AML CFT measures geographies	• % of high risk geographies based on FATF list of geographies with weak AML/CFT measures (e.g. in clients revenue, assets, transactions)
Clients/transactions	Volume	• Number of clients • Total number (stock) • New clients per year (flow)
	Risk	• % high risk clients (based on supervised entities' internal models) • % Politically exposed persons (PEPs) (over time): domestic vs. foreign
Channels	Channels	• Type of interaction: % face-to-face, indirect (e.g. online), via intermediaries
Typical ML/TF methods	Threats exposure	• Number of cases of predicate offences using this (sub-) sector
	ML/TF methods observed in Lux	• Number of cases identified (e.g. Suspicious transactions reports (STRs), convictions, examinations) • Luxembourg expert knowledge (e.g. case studies)
	Sector-specific ML/TF methods	• FATF guidance • Egmont Group case studies • Other countries (e.g. case studies, NRAs)

Vulnerability assessment: overview of inherent risk levels

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Sector	Sub-sector	2025 NRA: Inherent risk
Banks	Retail and business banks	High
	Entities operating online	High
	Wholesale, corporate and investment banks	High
	Private banking	Very High
	Custodians and sub-custodians (incl. Central Securities Depositories)	Medium
Investment sector	Investment firms authorized to carry out the services of investment advice and portfolio management[389]	High
	Investment firms authorized to carry out the services of reception and transmission of orders in relation to one or more financial instruments and of execution of orders on behalf of clients[390]	High
	Investment firms authorized to carry out activities of dealing on own account, of underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis and of placing financial instruments without a firm commitment basis[391]	Medium
	Collective investments	Medium
	CSSF-supervised pension funds	Low

Sector	Sub-sector	2025 NRA: Inherent risk
Money value or transfer services (MVTS)	Payment institutions (PIs)	High
	E-money institutions (EMIs)	High
	Agents and e-money distributors acting on behalf of PIs/EMIs established in other European Member States	Medium
VASPs		High
Specialised PFSs	Specialised PFSs providing corporate services	High
	Professional depositaries	Medium
Support PFSs and other specialised PFSs[392]	Support PFSs	Very Low
	Other specialised PFSs	
Market operators		Low
Insurance	Life insurance	High
	Non-life insurance	Low
	Reinsurance	Low
	Intermediaries	Medium
	Professionals of the insurance sector (PSAs)	Low
	CAA-supervised pension funds	Very Low

Vulnerability assessment: overview of inherent risk levels

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Sector	Sub-sector	2025 NRA: Inherent risk
Real estate agents and developers	Real estate agents *(agents immobiliers)*	High
	Real estate developers *(promoteurs immobiliers)*	High
Freeport operators	Freeport operators	Medium
Dealers in goods	Precious metals/jewellers/clocks	Medium
	Car dealers	High
	Art/Antiques	Medium
	Luxury goods (e.g. *"maroquinerie"*)	Medium
Gambling service providers	Casino	Medium
	National lottery	Low
Legal and accounting professions supervised by the AED	Accountants	High
	Professional directors and business centres	High

Sector	Sub-sector	2025 NRA: Inherent risk
Legal and accounting professions supervised by SRBs	Lawyers	High
	Notaries	High
	Court bailiffs *(Huissiers de justice)*	Medium
	Audit profession[393]	Medium
	Chartered professional accountants *(Experts-comptables)*	High
Legal persons and legal arrangements	*Sociétés commerciales*	Very High
	Sociétés civiles	Medium
	NPOs (as per FATF definition) carrying out primarily international activities – ASBLs and *Fondations*[394]	High
	NPOs (as per FATF definition) carrying out local activities – ASBLs[395]	Low
	NPOs (as per FATF definition) carrying out local activities – *Fondations*[396]	Low
	Other legal persons	High
	Domestic *Fiducies*	Very High
	Foreign trusts	Very High

Vulnerability assessment: Specialised PFSs providing corporate services

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Sector	Sub-sectors	2025 NRA: Inherent risk
Specialised PFSs	Specialised PFSs providing corporate services	High
	Professional depositaries	Medium
Support PFSs and other specialised PFSs[190]	Support PFSs	Very Low
	Other specialised PFSs	

Risk drivers (specialised PFSs providing corporate services)

- **Market structure and complexity:** Specialised PFSs sub-sector includes various licenses, each offering different services (registrar agents, corporate domiciliation agents, professionals providing company incorporation and management services and family offices)
- The **clientele** was almost entirely made up of legal persons with more than half of the client companies' BOs residing in non-EU countries, increasing ML risks
- Sub-sector provides **TCSP services**, which are deemed high risk from a ML perspective

What activities fall under the scope of trust and company service providers?

- ✓ Acting as a formation agent for legal entities
- ✓ Acting as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
- ✓ Providing a registered office, business address or accommodation, correspondence or administrative address
- ✓ Acting as a trustee of an express trust ore performing the equivalent function for another form of legal arrangement
- ✓ Acting as a nominee shareholder for another person

Vulnerability assessment: legal persons and legal arrangements

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

The analysis leverages on the methodology developed in the 2022 LPs/LAs VRA and updated data. This resulted in a more detailed, nuanced and data-based assessment

Sector	Sub-sectors	2025 NRA: Inherent risk
Legal persons and legal arrangements	*Sociétés commerciales*	Very High
	Sociétés civiles	Medium
	NPOs (as per FATF definition) carrying out primarily international activities – ASBLs and *Fondations*[266]	High
	NPOs (as per FATF definition) carrying out local activities – ASBLs[267] NEW	Low
	NPOs (as per FATF definition) carrying out local activities – *Fondations*[268]	Low
	Other legal persons	High
	Domestic *Fiducies*	Very High
	Foreign trusts	Very High

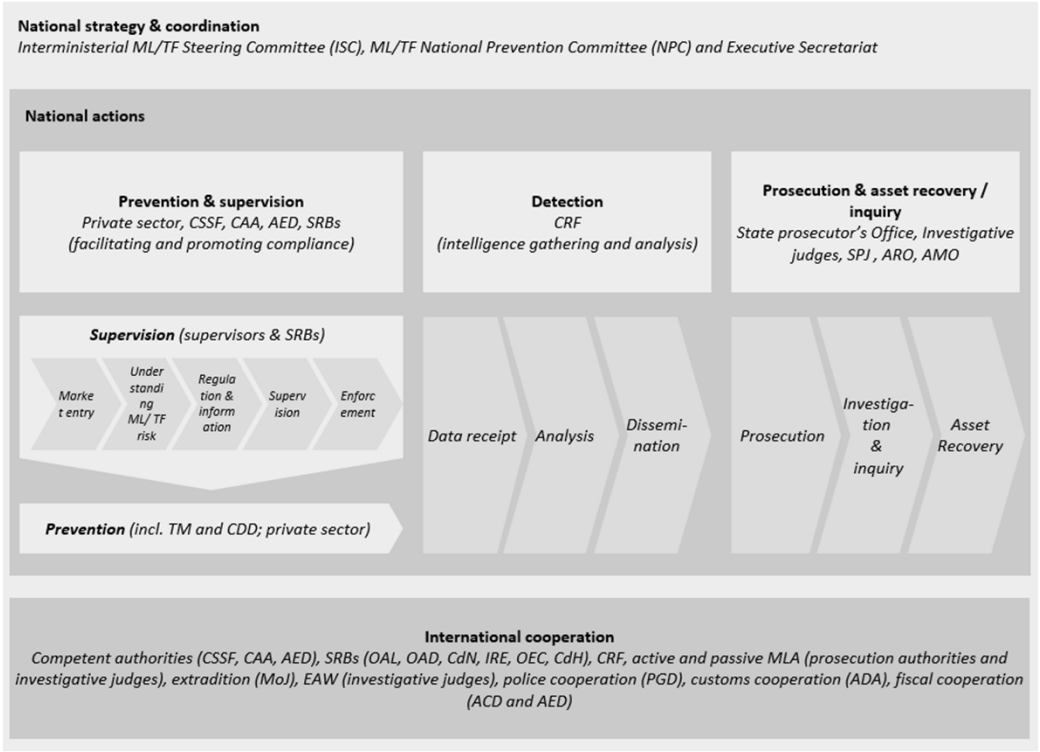
- The **2018 and 2020 NRA** assessed LPs/LAs as "High" risk, with *Sociétés commerciales*, followed by some NPOs bearing the highest inherent risk
- **2025 NRA ML**, the inherent risk levels remain roughly the same for all categories of legal persons (with the exception of "Other legal persons", assessed as High risk, in line with the **2022 LPs/LAs VRA**, and ASBLs falling under FATF NPO definition carrying out local activities, that have been assessed as Low risk)

Mitigating factors

National ML risk assessment 2025

Mitigating factors framework

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



These dimensions are reflected in the mitigating factors scorecards (cf. next slide)

Mitigating factors scorecard

This scorecard is used to assess the effectiveness of mitigating measures applied within each of the sub-sectors analysed in the context of the NRA exercise

Dimension	Criteria	Information/data used (examples)
Market entry controls	Market entry	• Licenses/registrations – number of applications received, processed, approved, rejected
	Breaches	• Number of licenses/registrations breaches identified / remediated
Understanding of ML/TF risks and AML/CFT obligations	Understanding of ML/TF risks and AML/CFT obligations	• Annual questionnaires • Risk assessments (e.g. entity level, sub-sector risk assessments) • Internal trainings • Supervisors' publications on ML/TF risks in the sector
	Regulation & information	• Type of supervisor (e.g. association, ministry, dedicated supervisor) • Regulation communication to the sector (e.g. circulars) • Education to private sector (e.g. publications, trainings, etc.)
Prevention / Private sector controls	ML/TF controls in place	• CDD / KYC approach, aligned with risk level, number of customers declined based on CDD • Transaction monitoring approach, aligned with risk level, number of alerts generated, handled and STRs reported
	Internal supporting structures	• Formalised policies, procedures and controls, clearly articulating the risk-based AML/CFT approach • Member of management body responsible for compliance with AML/CFT obligations
Supervision & enforcement	Level of supervision	• Number and type of inspections (on-sites and off-sites) • Supervisor procedures formalised and up to date
	Enforcement	• Remedial actions imposed (i.e. number of sanctions and other actions) • Outcomes of remedial actions (i.e. number of deficiencies remediates)
Detection, Prosecution & asset recovery	STRs/SARs	• Number of STRs and SARs issued by subsector and predicate offences • Quality of STRs and SARs issued by subsector and predicate offences
	FIU analyses	• Number of FIU analyses by subsector and predicate offence
	Investigations / prosecution / convictions	• Number of investigations/prosecutions/convictions against subsector entities by subsector and predicate offence
	Seizures / confiscations	• Number of seizures/confiscations and total value by subsector and predicate offence

Residual risk assessment

National ML risk assessment 2025

Residual risk assessment

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Sector	Sub-sector	2025 NRA: Inherent risk	2025 NRA: Residual risk
Banks	Retail and business banks	High	Medium
	Entities operating online	High	Medium
	Wholesale, corporate and investment banks	High	Medium
	Private banking	Very High	Medium
	Custodians and sub-custodians (incl. Central Securities Depositories)	Medium	Low
Investment sector	Investment firms authorized to carry out the services of investment advice and portfolio management[389]	High	Medium
	Investment firms authorized to carry out the services of reception and transmission of orders in relation to one or more financial instruments and of execution of orders on behalf of clients[390]	High	Medium
	Investment firms authorized to carry out activities of dealing on own account, of underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis and of placing financial instruments without a firm commitment basis[391]	Medium	Low
	Collective investments	Medium	Medium
	CSSF-supervised pension funds	Low	Very Low

Residual risk assessment

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Sector	Sub-sector	2025 NRA: Inherent risk	2025 NRA: Residual risk
Money value or transfer services (MVTS)	Payment institutions (PIs)	High	Medium
	E-money institutions (EMIs)	High	Medium
	Agents and e-money distributors acting on behalf of PIs/EMIs established in other European Member States	Medium	Medium
VASPs		High	Medium
Specialised PFSs	Specialised PFSs providing corporate services	High	Medium
	Professional depositaries	Medium	Low
Support PFSs and other specialised PFSs[392]	Support PFSs	Very Low	Very Low
	Other specialised PFSs		
Market operators		Low	Low
Insurance	Life insurance	High	Medium
	Non-life insurance	Low	Low
	Reinsurance	Low	Low
	Intermediaries	Medium	Low
	Professionals of the insurance sector (PSAs)	Low	Very Low
	CAA-supervised pension funds	Very Low	Very Low

Residual risk assessment

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Sector	Sub-sector	2025 NRA: Inherent risk	2025 NRA: Residual risk
Real estate agents and developers	Real estate agents *(agents immobiliers)*	High	Medium
	Real estate developers *(promoteurs immobiliers)*	High	Medium
Freeport operators	Freeport operators	Medium	Low
Dealers in goods	Precious metals/jewellers/clocks	Medium	Low
	Car dealers	High	Medium
	Art/Antiques	Medium	Low
	Luxury goods (e.g. *"maroquinerie"*)	Medium	Medium
Gambling service providers	Casino	Medium	Very Low
	National lottery	Low	Very Low
Legal and accounting professions supervised by the AED	Accountants	High	High
	Professional directors and business centres	High	High

Residual risk assessment

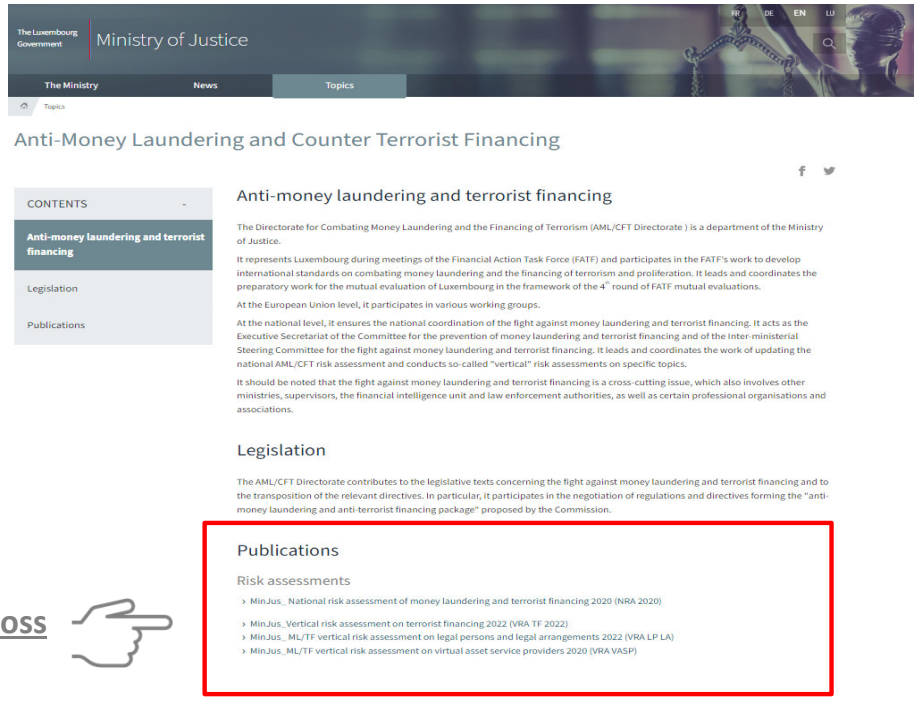
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Sector	Sub-sector	2025 NRA: Inherent risk	2025 NRA: Residual risk
Legal and accounting professions supervised by SRBs	Lawyers	High	Medium
	Notaries	High	Medium
	Court bailiffs *(Huissiers de justice)*	Medium	Medium
	Audit profession[393]	Medium	Low
	Chartered professional accountants *(Experts-comptables)*	High	Medium
Legal persons and legal arrangements	*Sociétés commerciales*	Very High	Medium
	Sociétés civiles	Medium	Low
	NPOs (as per FATF definition) carrying out primarily international activities – ASBLs and *Fondations*[394]	High	High
	NPOs (as per FATF definition) carrying out local activities – ASBLs[395]	Low	Low
	NPOs (as per FATF definition) carrying out local activities – *Fondations*[396]	Low	Very Low
	Other legal persons	High	Medium
	Domestic *Fiducies*	Very High	Very High
	Foreign trusts	Very High	Very High

Conclusion

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

The NRA plays a central role in the national AML/CFT framework and may assist AML/CFT obliged entities in conducting their own risk assessment and in the application of a risk-based approach



https://mj.gouvernement.lu/en/dossiers/2020/lutte-blanchiment.html