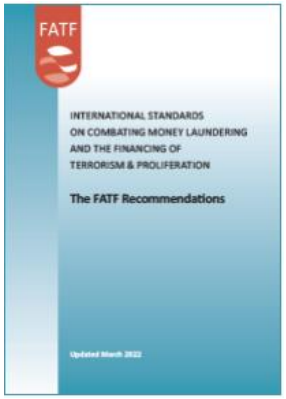
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Justice

Terrorist financing
vertical risk assessment

May 2022

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

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 keypoints 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.

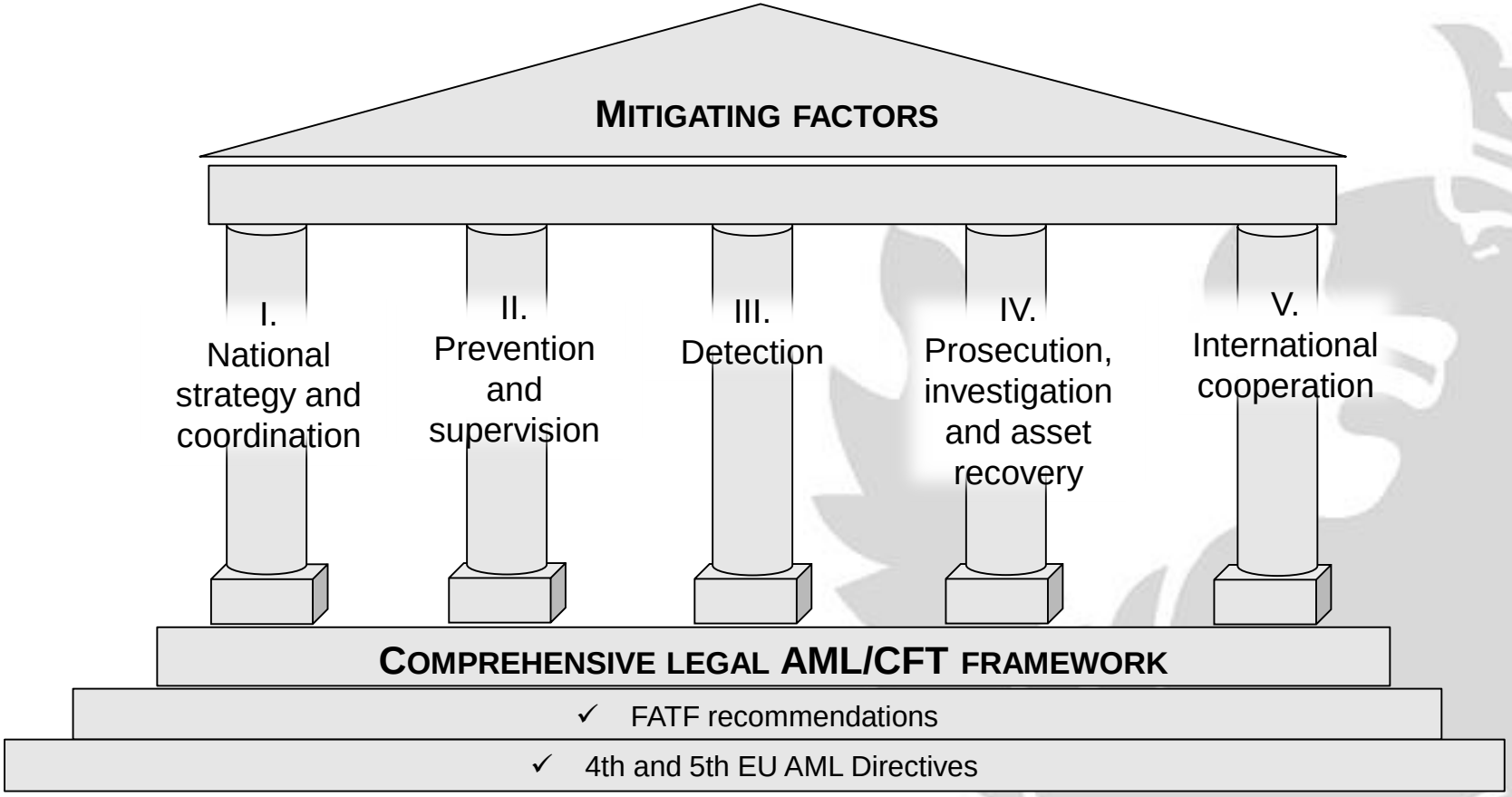
- Although the **2019 European Supranational risk assessment** (link) recognised the risks of virtual assets being misused to finance terrorism as emerging…
- … a more recent report from **Europo**l (2021) (link) states that the number of cases involving virtual assets for TF remains limited.
- As of 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. Mitigation 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

6. Questions?

Thank you for your attention!