



Evaluation verticale des risques **Financement du terrorisme**

Mai 2022





1. Introduction
2. Approche et méthodologie
3. Risque inhérent: menaces et vulnérabilités
4. Facteurs atténuants et risque résiduel
5. Conclusions
6. Questions





1. Introduction



- Les recommandations du GAFI ([lien](#)):
 - La **R.1** sur l'évaluation des risques et l'application d'une approche fondée sur les risques et sa **note interprétative** indique que « *Les pays devraient identifier, évaluer et comprendre les risques de blanchiment de capitaux et de financement du terrorisme auxquels ils sont exposés [...]* »
 - La **R.8** sur les organismes à but non lucratif (OBNL) et sa **note interprétative** indique que « *Les pays devraient examiner la pertinence de leurs lois et règlements relatifs aux organismes à but non lucratif qu'ils ont identifiés comme vulnérables à une exploitation à des fins de financement du terrorisme. Les pays devraient appliquer des mesures ciblées et proportionnées à ces OBNL, selon une approche basée sur les risques, pour les protéger d'une exploitation à des fins de financement du terrorisme [...]* »
- L'actualisation de l'**Evaluation nationale des risques (ENR 2020)** ([lien](#)) a conclu que les risques de financement du terrorisme (FT) sont globalement modérés. Alors que l'ENR couvre à la fois le blanchiment de capitaux (BC) et le FT, l'**Evaluation verticale de risques du FT** se concentre spécifiquement sur le FT. Aussi l'évaluation verticale approfondi l'examen des risques de FT posés sur les OBNL.

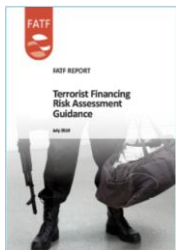




2. Approche et méthodologie (1/2)

- ? Comment élaborer une évaluation de risque de FT dans un pays sans organisation terroriste opérant dans son territoire?
- ? Comment tenir compte de la présence du centre financier?

→ Référence de base: FATF, *Terrorist financing assessment guidance*, 2019, §39 ([link](#)).



☞ Evaluer les risques de FT dans les pays dotés de centres financiers et présentant un faible risque domestique de terrorisme

Périmètre: l'évaluation verticale de risque de FT couvre les trois étapes du FT



Point de départ: **terrorisme** (analyse du contexte, des acteurs, de leurs attaques, de leurs besoins)

└─> **financement du terrorisme**



2. Approche et méthodologie (2/2)

1) Evaluation des différents **types d'acteurs terroristes** et classement en fonction de leurs **besoins** financiers au cours des différentes étapes du FT (la collecte, le déplacement et l'utilisation):

- Petites cellules, acteurs isolés et combattants terroristes étrangers: faibles besoins financiers.
- Organisations terroristes internationales et leurs sponsors: besoins financiers plus importants.

2) Analyse des **attaques terroristes dans les pays avec qui le Luxembourg a des liens**, soit de par sa situation géographique (Union Européenne (UE), incl. le Royaume-Uni), soit de par son centre financier (pays tiers):

- Analyse de l'exposition au risque de FT découlant des acteurs isolés et des petites cellules opérant au sein de l'UE et du Royaume-Uni (ISIL et d'extrême droite en moindre mesure): mouvement de fonds modestes qui transitent par des services tels que la banque de détail et le secteur des services de valeurs ou de fonds (MVTs).
- Analyse du risque de FT qui représentent les flux de fonds plus importants vers ou en provenance d'organisations terroristes étrangères (p.ex. ISIL) et qui transitent par la place financière de Luxembourg.

3) Une **analyse sectorielle** est menée en 2 étapes (même approche que l'ENR 2020, avec des ajustements spécifiques):

1. Evaluation du RISQUE INHÉRENT
(menaces x vulnérabilités)

2. Evaluation des
FACTEURS ATTÉNUANTS

RISQUE
RÉSIDUEL



3. Risque inhérent – menaces (1/2)

Contexte européen:

Attentats perpétrés en majorité par de **petites cellules ou des acteurs isolés** liés à l'État islamique d'Irak et du Levant (ISIL) (et par des terroristes d'extrême droite en moindre mesure). Même si ces attaques ont été assez nombreuses, leur préparation et leur exécution ont nécessité **peu de moyens financiers**.

En outre, **les combattants terroristes étrangers (CTE)** provenant des Etats membres de l'UE demeurent une source de préoccupation.

Implications pour la place financière du Luxembourg:

→ Principale menace liée aux acteurs isolés et aux petites cellules:

- Exploitation et utilisation abusive de produits financiers proposés par des entités basées au Luxembourg pour collecter, acheminer et dépenser de petites sommes d'argent à des fins de FT. Essentiellement, des services financiers de base offerts aux clients locaux et européens par les banques de détail et d'affaires, les établissements de paiement et de monnaie électronique.
- Le Luxembourg est exposé à ce type de risque en raison du nombre important d'entités fournissant ces services (et non en raison d'un risque plus élevé de ses services de bases offerts ici par rapport à ailleurs).

→ Principale menace liée aux CTE sortant ou entrant des zones de conflits:

- Retrait d'argent de comptes luxembourgeois par le biais de distributeurs automatiques de billets (DAB) situés à proximité des zones de conflit en Syrie, en Iran ou en Irak.

☞ Toutes les institutions financières luxembourgeoises sont entièrement réglementées et supervisées aux fins de la LBC/FT par la CSSF.

☞ Maturité du secteur financier et sensibilisation pour la prévention du FT significatives.



3. Risque inhérent – menaces (2/2)

Contexte dans des pays tiers avec une menace terroriste active:

Alors qu'ISIL opère dans l'UE principalement par le biais d'acteurs isolés et de petites cellules terroristes, il opère en tant qu'**organisation terroriste internationale** dans les refuges que constituent les vastes régions désertiques du Sahara ou les régions semi-désertiques du Sahel. D'un point de vue quantitatif, les **besoins en matière de FT** pour l'ISIL et ses affiliés **dans ces régions** sont **très élevés**.

Implications pour la place financière du Luxembourg:

→ Principales menaces posées par les organisations terroristes et leurs sponsors fortunés:

- Utilisation de la place financière pour acheminer des fonds plus importants en provenance ou à destination d'organisations terroristes internationales établies dans des régions particulièrement touchées par le terrorisme. Ceci menace les sous-secteurs les plus sophistiquées du secteur financier, principalement la banque privée et le secteur de l'investissement.
- Collecte de fonds (dons de résidents luxembourgeois) à des organisations à but non lucratif (OBNL) réalisant des projets de développement et humanitaires à l'étranger et acheminement (en envoyant des fonds à des organisations terroristes internationales en abusant des services offerts par la place financière et adaptés à des besoins financiers élevés en matière de FT).

- ☞ L'exposition du Luxembourg à ces menaces a été évaluée notamment par l'analyse des flux financiers et non financiers en provenance et à destination d'une sélection de juridictions pertinentes issus des régions précitées.
- ☞ Les flux analysés s'inscrivent dans le cadre des relations bilatérales. Le volume et la nature de ces flux n'ont pas révélé de menace concrète pour la place financière du Luxembourg en matière de FT.



3. Risque inhérent – vulnérabilités (1/6)

VULNÉRABILITÉS SECTORIELLES:

Organisations à but non-lucratif

- Globalement, les organisations à but-non lucratif (OBNL) réalisant des projets de développement et humanitaires à l'étranger sont exposés à deux points clés de leurs opérations : par les dons qu'ils reçoivent et par la destination de leurs fonds.
- Bien que ces typologies observées au niveau mondial n'aient pas été détectées, les OBNL luxembourgeoises réalisant des projets de développement et humanitaires à l'étranger restent vulnérables compte tenu de la localisation de leurs activités.

Sous-secteur de la banque de détail et de la banque des affaires

- Les produits bancaires traditionnels offerts par les banques de détail et les banques d'affaires (par ex: les cartes de débit/crédit, les virements électroniques, les retraits aux guichets automatiques) les rendent vulnérables aux attaques d'acteurs isolés, des petites cellules terroristes ou des CTE.
- Les activités de la banque de détail au Luxembourg se concentrent sur une clientèle locale:



Selon une enquête récente menée par la CSSF et l'ABBL sur l'activité de banque de détail ([lien](#)), la majorité des actifs et passifs sont détenus par des résidents nationaux (88%).

- Les banques de détail et d'affaires ont déposé le plus grand nombre de déclarations de soupçon : 22 TFAR en 2020 (8 en 2019) et 4 TFTR en 2020 (14 en 2019) ([lien](#)).



3. Risque inhérent – vulnérabilités (2/6)

Secteur des services de transferts de fonds et de valeurs

- Comme pour les activités issues de la banque de détail et d'affaires, les produits et services proposés par le secteur des services de transferts de fonds et de valeurs permettent un accès facile, rapide et pratique à des transactions transfrontalières. Cela rend le secteur vulnérable aux abus de la part d'acteurs isolés et de petites cellules opérant dans l'UE ainsi que par des CTE.
- La taille et le volume des transactions des sous-secteurs luxembourgeois des établissements de paiement et des établissements de monnaie électronique sont importants, alors que seuls quelques agents/distributeurs de monnaie électronique, agissant pour le compte d'établissements de paiement/établissements de monnaie électronique établis dans d'autres États membres de l'UE, opèrent au Luxembourg



3. Risque inhérent – vulnérabilités (3/6)

Sous-secteur de la banque privée

- L'exposition des banques privées au FT est déterminée par leur taille, leur exposition internationale et la nature de leurs clients (c'est-à-dire la prédominance de comptes potentiellement plus sophistiqués).
- Le seuil financier requis pour entamer une relation d'affaires et les liens étroits avec les clients (par exemple, les produits sont conçus pour une relation à long terme, le recours à des gestionnaires de clientèle) rendent la banque privée peu attrayante pour les acteurs ayant de faibles besoins financiers.
- Cependant, des financiers du terrorisme pourraient conclure des contrats de gestion d'actifs ou de patrimoine avec des banques privées luxembourgeoises en vue d'héberger leurs actifs, même si les actifs ou le patrimoine gérés au Luxembourg ne sont pas directement liés au FT.

Secteur de l'investissement

- Comme pour le sous-secteur de la banque privée, l'exposition du secteur de l'investissement au FT semble plus importante pour les financeurs du terrorisme en dehors de l'UE que pour les acteurs isolés ou les petites cellules terroristes opérant au sein de l'UE. Cela est particulièrement vrai pour le sous-secteur de la gestion de patrimoine et d'actifs, qui s'adresse généralement à des particuliers fortunés.
- Néanmoins, il n'y a que peu de preuves que le secteur de l'investissement soit utilisé à des fins de FT, comme le montre le très faible nombre de TFTR/TFAR. Il n'empêche que, comme pour le secteur de la banque privée, la taille du secteur de l'investissement est considérée comme un facteur de vulnérabilité.



3. Risque inhérent – vulnérabilités (4/6)



Dans le secteur de la banque privée et de l'investissement, les décisions d'investissement peuvent être prises discrétionnairement (les décisions d'investissement sont prises par le professionnel et non par le client). Il est donc peu probable que les fonds soient « acheminés » ou « utilisés » à des fins de FT dans ces (sous-) secteurs. Ainsi, il est essentiel de faire la distinction entre les investissements réalisés par le professionnel pour le compte de son client, qui sont en principe indisponibles, et l'utilisation des plus-values qui sont à la disposition de son client, sauf si elles sont réinvesties.



3. Risque inhérent – vulnérabilités (5/6)

VULNÉRABILITÉS TRANSVERSALES: ARGENT LIQUIDE ET NOUVELLES TECHNOLOGIES

Argent liquide

- Globalement, l'argent liquide est le mode de transport le plus fréquemment utilisé à des fins criminelles, y compris le FT.
- La Turquie est considérée comme une plaque tournante importante pour les CTE en raison de sa localisation géographique.
- Les risques de FT résultant de l'utilisation d'argent liquide au Luxembourg doivent être prises en considération par les entités publiques et privées.

- ☞ Cependant, Luxembourg n'a pas détecté de groupes terroristes opérant sur son sol et il n'y a pas de preuves connues de collecte d'argent liquide à des fins de FT au Luxembourg.
- ☞ L'analyse de retraits de sommes déposés dans des banques luxembourgeoises depuis des distributeurs situés en Turquie près des frontières syrienne, iranienne et irakienne montre que ceux-ci étaient plutôt limités et qu'aucune preuve suggérait qu'ils puissent être en lien avec le FT ou des CTE.



3. Risque inhérent – vulnérabilités (6/6)

Nouvelles technologies



- Selon un rapport récent publié par le **Royal United Services Institute** ([lien](#)):
 - (i) Il apparaît que les nouvelles technologies (par ex: les médias sociaux et le *crowdfunding*, les actifs virtuels) n'ont pas joué un rôle prédominant dans le financement de la plupart des attaques terroristes européennes (c.-à-d. celles menées par des acteurs isolés et des petites cellules)
 - (ii) De manière générale, il a été observé que les groupes terroristes utilisaient les actifs virtuels, le *crowdfunding* basé sur les dons, les médias sociaux et les fournisseurs de services de paiement, en particulier dans les phases de collecte et d'acheminement.
 - (iii) Néanmoins, les nouvelles technologies se sont ajoutées aux méthodes de FT traditionnelles plutôt que de les remplacer.
- Bien que l'**Evaluation supranationale des risques (2019)** réalisé par la Commission européenne ([lien](#)) ait reconnu que les risques d'utilisation abusive des actifs virtuels pour financer le terrorisme étaient émergents...
- ... un rapport plus récent d'**Europol (2021)** ([lien](#)) indique que le nombre de cas impliquant des actifs virtuels pour le TF reste limité.
- Au 31 décembre 2021, le Luxembourg compte six prestataires de services d'actifs virtuels (PSAV) enregistrés. Six TFTR/TFAR ont été reportés par des entités liées aux actifs virtuels ou aux PSAV à la Cellule de renseignement financier (CRF) en 2020 et 29 en 2021. Rien n'indique que les PSAV luxembourgeois soient exposés de manière significative au FT.



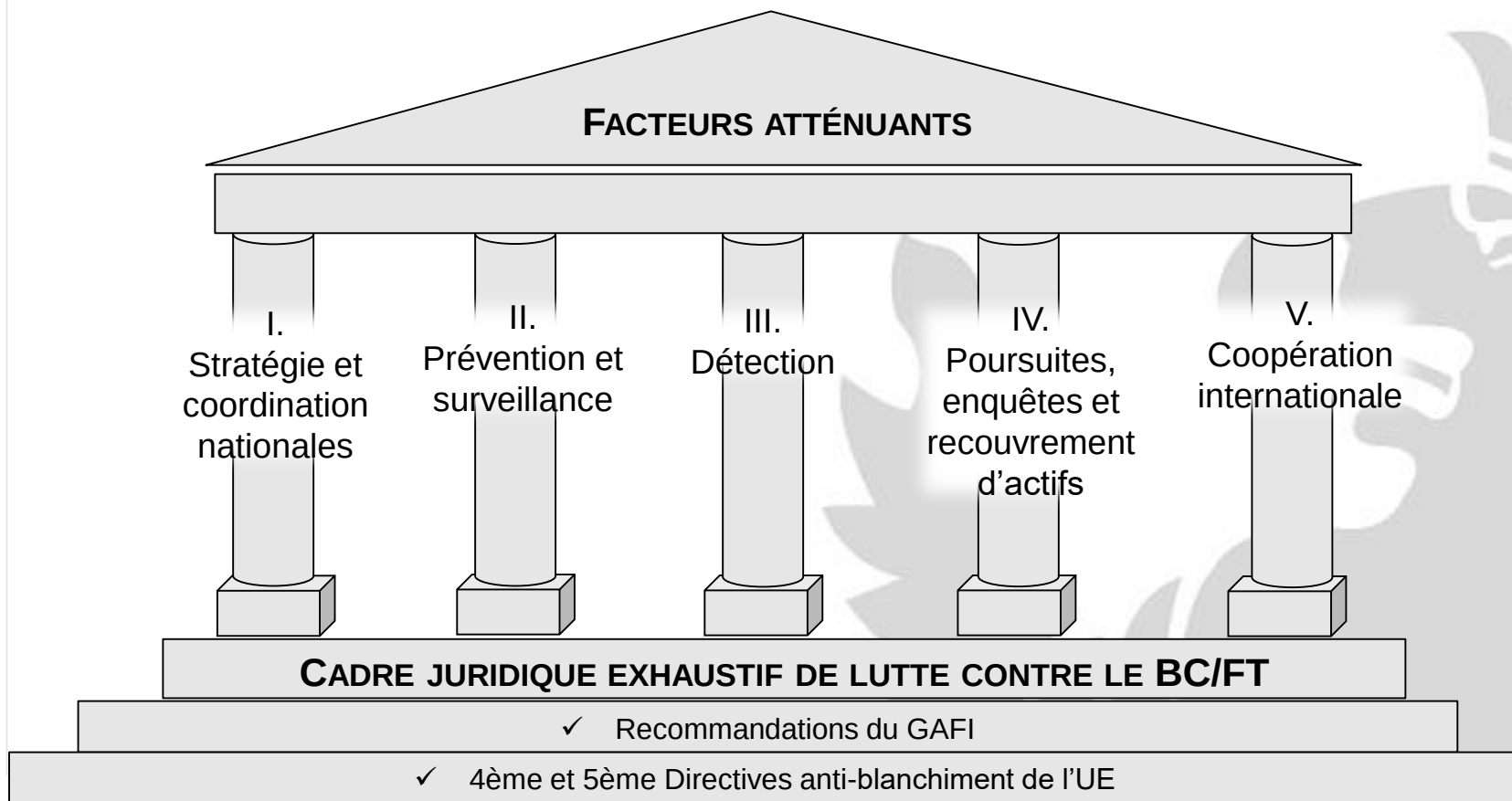


4. Facteurs atténuants et risque résiduel

1. Evaluation du RISQUE INHÉRENT
(menaces x vulnérabilités)

2. Evaluation des
FACTEURS ATTÉNUANTS

RISQUE
RÉSIDUEL





4. Facteurs atténuants et risque résiduel

Secteur	Sous-secteur	Risque inhérent de TF		Risque résiduel de TF
Banques	Banque privée	Moyen	Impact des facteurs d'atténuation	Faible
	Banques de détail et d'affaires	Haut		Moyen
Secteur de l'investissement	Gestionnaires de patrimoine et d'actifs	Moyen		Faible
	Placements collectifs	Moyen		Faible
Services de transferts de fonds et de valeurs	Établissements de paiement (EP)	Haut		Moyen
	Institutions de monnaie électronique (IME)			
	Agents et distributeurs de monnaie électronique agissant pour le compte de EP/EMI établis dans d'autres États membres européens			
OBNL réalisant des projets de développement et d'aide humanitaire à l'étranger	OBNL (Associations sans but lucratif et fondations) réalisant des projets de développement et d'aide humanitaire à l'étranger	Haut	Haut	



5. Conclusions (1/2)

Pour conclure, le tableau suivant résume, pour chaque étape du FT, le risque résiduel de FT des différents (sous-)secteurs évalués.

	Collecte	Acheminement	Utilisation
Banque de détail et d'affaires	Les petites cellules, les acteurs isolés et les CTE peuvent collecter des fonds d'origine légitime (par ex : salaires, prestations sociales, prêts, découverts).	Les services financiers de base (par ex : virements électroniques, retraits aux guichets automatiques) peuvent être abusés pour transférer des fonds destinés au terrorisme vers des petites cellules, des acteurs isolés et des CTE.	Les petites cellules, les acteurs isolés et les CTE peuvent utiliser des fonds pour commettre des actes terroristes.
Banque privée et Secteur de l'investissement	Pertinence pour les financeurs du terrorisme en dehors de l'UE.	La gestion d'actifs discrétionnaire ne convient pas pour transférer des fonds à des fins de TF. Les fonds gérés par le gestionnaire d'actifs dans le cadre d'un contrat discrétionnaire sont inaccessibles au client. Les revenus générés qui ne font plus l'objet d'une gestion discrétionnaire peuvent être transférés à des terroristes ou à des organisations terroristes.	Non applicable tant que les fonds sont sous gestion discrétionnaire. Cela n'empêche pas le secteur de l'investissement d'exercer le devoir de vigilance (renforcée) sur les projets d'investissement dans les régions touchées par le terrorisme et sur les personnes morales opérant dans ces régions.



5. Conclusions (2/2)

(suite)	Collecte	Acheminement	Utilisation
Services de transferts de fonds et de valeurs	Les petites cellules, les acteurs isolés et les CTE peuvent abuser de ces prestataires pour collecter des fonds à des fins de FT (y compris les paiements liés aux services de <i>crowdfunding</i>).	Ces prestataires peuvent être abusés pour transférer des fonds destinés au FT vers des petites cellules, des acteurs isolés et des CTE.	Les petites cellules, les acteurs isolés et les CTE peuvent utiliser des fonds pour commettre des actes terroristes.
OBNL réalisant des projets de développement et d'aide humanitaire à l'étranger	Les OBNL peuvent collecter des fonds (de manière délibérée ou par inadvertance) à des fins de FT	Certains pays à haut risque n'ont qu'un accès limité aux systèmes de correspondants bancaires internationaux et certains OBNL menant des projets de développement et d'aide humanitaire à l'étranger peuvent être tentés d'utiliser des canaux informels ou non réglementés (par ex: <i>Hawala</i> ou autres) pour transférer des fonds vers ces pays. Aucune preuve de l'existence de <i>Hawala</i> ou d'autres prestataires de services opérant au Luxembourg.	Non applicable, sauf pour les OBNL qui collectent, de manière intentionnelle, des fonds à des fins de FT.



6. Questions





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

Merci de votre attention!

