Session « AML Tuesday's » n° 42 concernant les :

Risques LCB/FT évolutifs

5 décembre 2023

Sujets abordés

01 Type de risques émergents de blanchiment de capitaux

02 Risques émergents de financement du terrorisme

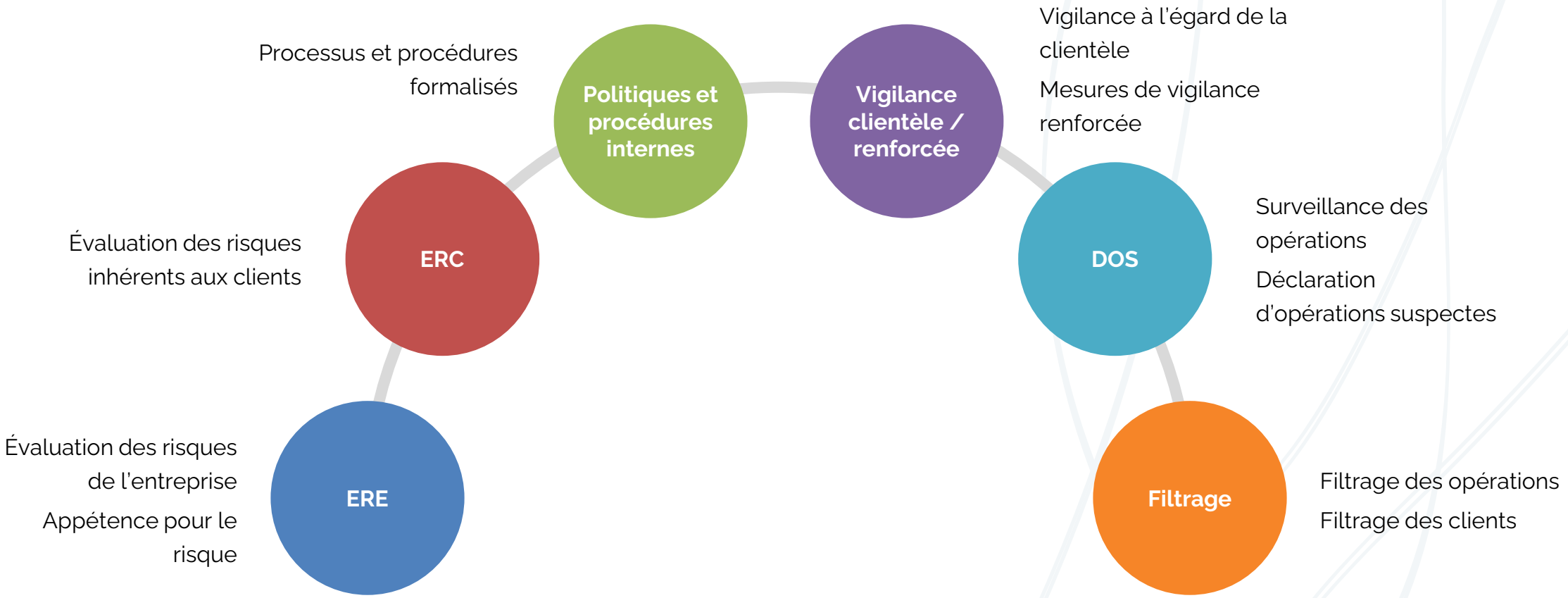
03 Comment le secteur privé peut-il identifier les risques émergents ?

04 Ce qu'il faut faire en pratique

Caractéristiques des risques émergents

- Manifestations à grande échelle
- Découlent souvent de tendances globales
- Échappent aux dispositifs de contrôle
- Peuvent dépasser les frontières géographiques, les industries et les secteurs
- Leur impact est difficile à quantifier
- Sont difficiles à prévoir
- Les méthodes traditionnelles d'identification et d'évaluation de la gestion des risques peuvent s'avérer inefficaces

Gestion des risques LCB/FT – Contrôles clés



Risques émergents – Blanchiment de capitaux

Développement technologique

Ukraine – Sanctions contre la Russie

Label blanc de l'ABE

IBAN virtuels de l'ABE

Risques de criminalité environnementale

Risque émergent – Blockchain/actifs virtuels

Vitesse de transaction élevée	Portée mondiale	Principauté	Anonymat
Possibilité de contourner les autorités centrales de régulation et de poursuite pénale	Type d'actifs – monnaies confidentielles	Jetons non fongibles NFT	Cryptoactifs

Contournement des sanctions contre la Russie – Signaux d'alerte

- L'utilisation de véhicules d'investissement communs dans le secteur de l'immobilier commercial – Alerte FinCen
- L'utilisation d'un véhicule d'investissement privé basé à l'étranger pour acquérir de l'immobilier commercial et qui inclut des PPE ou d'autres ressortissants étrangers (en particulier des membres de la famille ou des associés proches des élites russes sanctionnées et de leurs mandataires) en tant qu'investisseurs.
- Plusieurs sociétés à responsabilité limitée, sociétés anonymes, sociétés de personnes ou trusts sont impliquées dans une transaction ayant des liens avec les élites russes sanctionnées et leurs mandataires, et le nom des entités présente de légères variations.
- L'utilisation de personnes morales ou de constructions juridiques (trusts, par exemple) pour acquérir de l'immobilier commercial en impliquant des amis, des associés, des membres de la famille ou d'autres personnes ayant un lien étroit avec les élites russes sanctionnées et leurs mandataires.
- Détention d'actifs immobiliers commerciaux par l'intermédiaire d'entités juridiques dans plusieurs juridictions, sans objectif commercial clair.
- Les fonds d'investissement privés ou autres sociétés qui soumettent aux institutions financières des déclarations de propriété révisées montrant que des personnes sanctionnées ou des PPE qui détenaient auparavant plus de 50 % d'un fonds ont modifié leur participation pour la ramener à moins de 50 %.
- L'achat, la vente, la donation ou le transfert légal de propriété de biens immobiliers de grande valeur au nom d'une entité juridique étrangère, d'une société-écran ou d'un trust, en particulier si la transaction : (i) est largement supérieure ou inférieure à la juste valeur marchande, (ii) implique des transferts entièrement en espèces, ou (iii) est financée par un tiers ayant un lien connu avec les élites russes sanctionnées et leurs mandataires.
- Transactions impliquant des sociétés commerciales de PMSJ, en particulier en Asie, et des entreprises ayant un lien avec les élites russes sanctionnées et leurs mandataires.

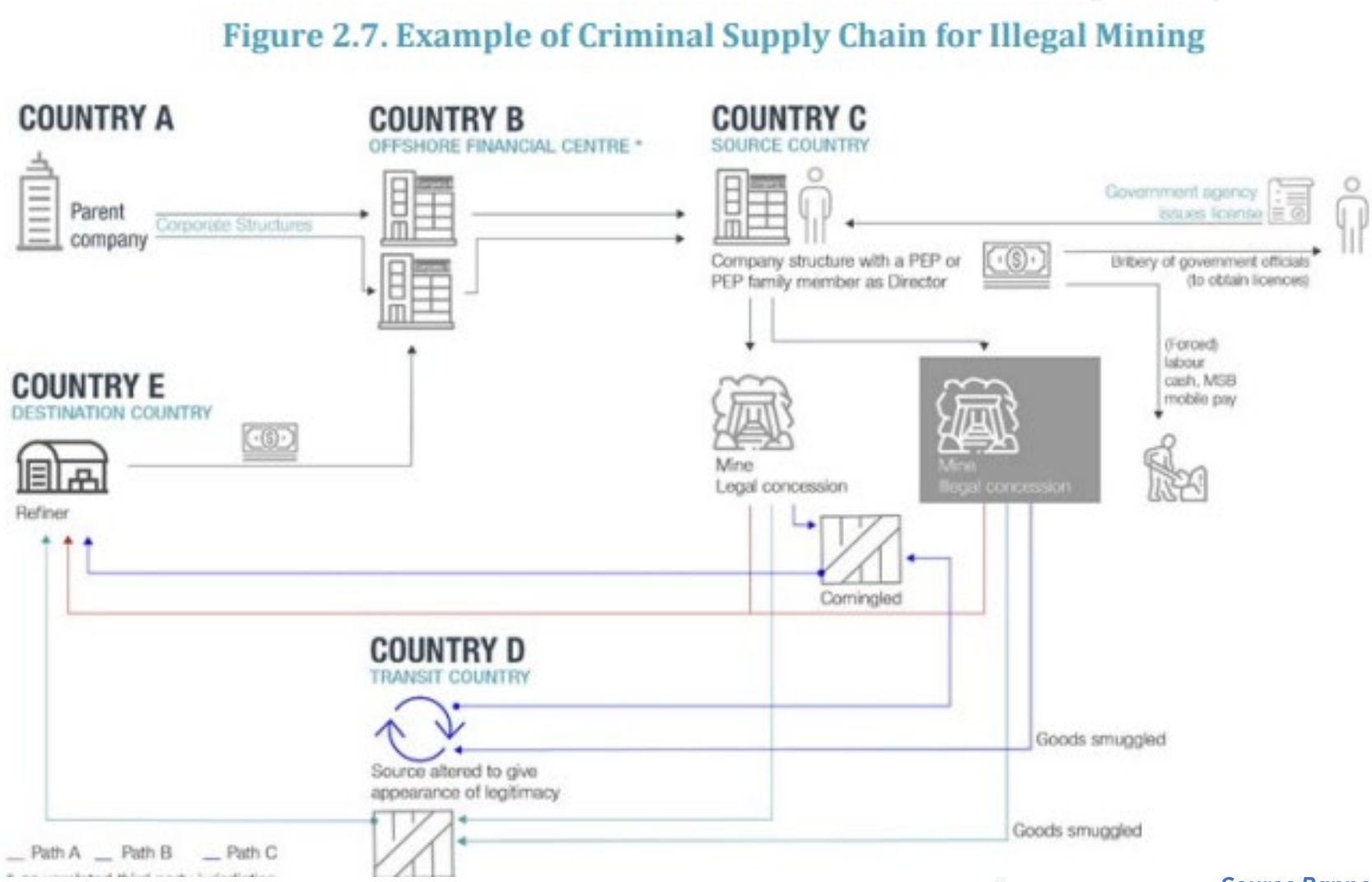
Risques de criminalité environnementale

- En l'absence de définition universelle de la criminalité environnementale, ce concept désigne généralement des infractions pénales portant atteinte à l'environnement, notamment l'exploitation forestière illégale, le défrichement illégal, l'exploitation minière illégale et le trafic de déchets.
- La criminalité environnementale est une entreprise criminelle très rentable, qui génère chaque année des produits de l'ordre de 110 à 281 milliards de dollars.
- Ces activités deviennent illégales si : (i) elles sont entreprises sans l'autorisation de l'État, (ii) les contrats et les concessions sont obtenus par la corruption ou l'intimidation, (iii) les services impliquent une fraude (p. ex. un faux traitement de déchets dangereux), et (iv) en matière d'exploitation forestière/minière, l'extraction contrevient aux conditions convenues, notamment quotas ou autres exigences.

Risques de criminalité environnementale – Signaux d'alerte

- Utilisation de sociétés-écrans pour mélanger produits illégaux et légaux.
- Utilisation de sociétés-écrans pour dissimuler des bénéficiaires effectifs.
- Transferts d'un pays où se trouvent des fonderies d'or vers des pays sources d'or, et retrait presque immédiat en espèces de la majeure partie du transfert.
- Sociétés opérant dans le secteur de l'exploitation forestière et effectuant fréquemment des transactions avec des centres financiers à l'étranger.
- Des personnes et des entités sont citées dans des journaux, des rapports d'enquête d'OBNL ou des rapports d'organisations internationales (publics et confidentiels) comme étant impliquées dans des affaires de pots-de-vin, de corruption, de crimes contre l'environnement ou d'autres infractions relevant du crime organisé.
- Clients disposant de permis d'exploitation minière et opérant dans ou autour de zones de conflit actif.
- Personne identifiée comme gérant ou administrateur de plusieurs entreprises liées à l'extraction environnementale.

Risques de criminalité environnementale



Source Rapport du GAFI – Blanchiment de capitaux issus de la criminalité environnementale

Risques émergents – FT

Financement du terrorisme

- Collecte de fonds au moyen des réseaux sociaux
- Collecte de fonds liés au terrorisme par financement participatif (crowdfunding)
- Collecte de fonds en monnaies virtuelles
- Organisations caritatives et fondations

Collecte

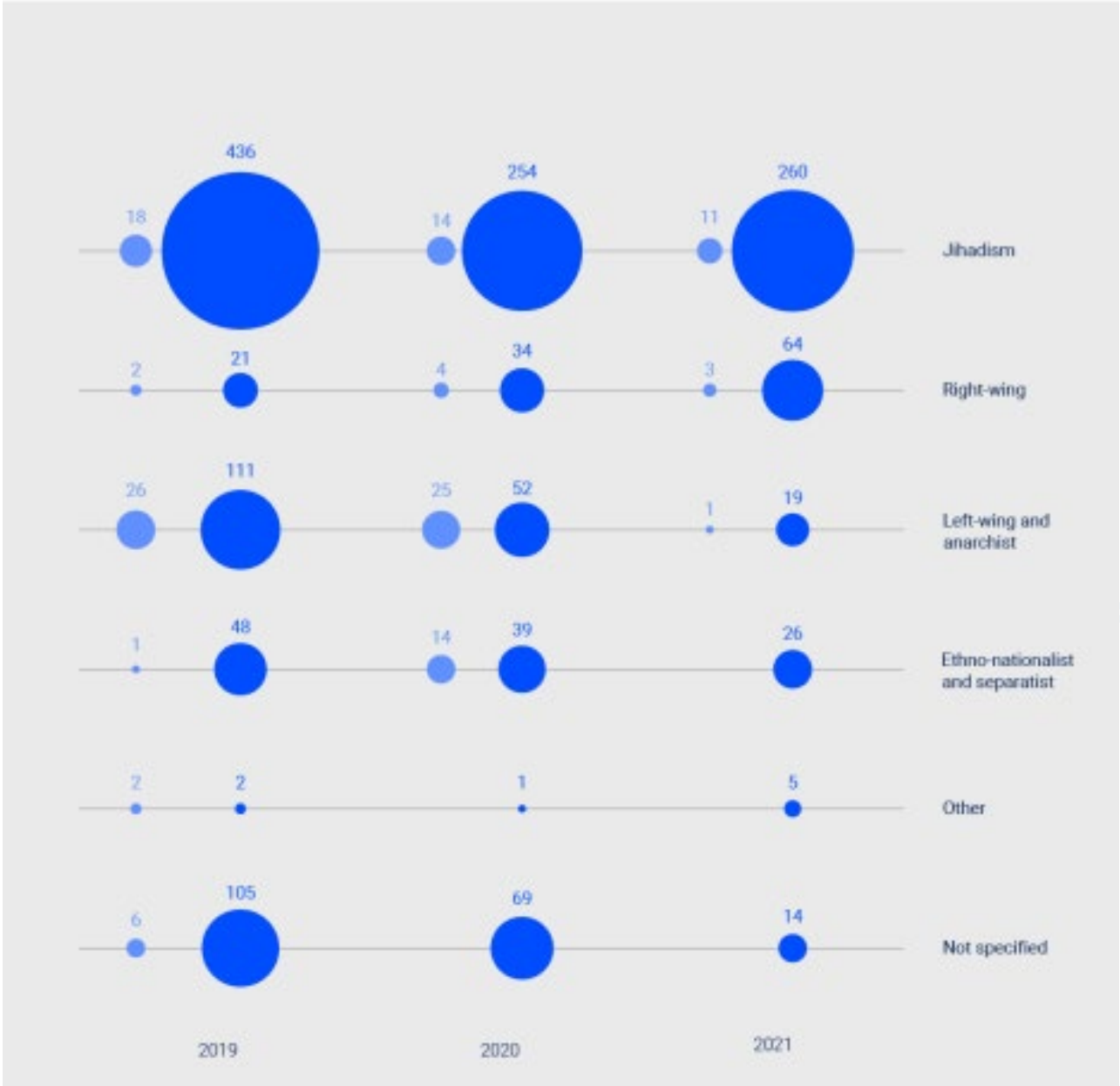
- Transbordement de marchandises
- Contrebande d'espèces
- Transferts de fonds de/vers des juridictions touchées par le terrorisme ou considérées comme des zones sensibles du terrorisme

Mouvement

- Attaque terroriste
- Entretien de réseaux et infrastructures terroristes
- Investissement de fonds liés au terrorisme

Utilisation

Attaques terroristes
réalisées, déjouées, manquées,
et arrestations pour suspicion
de
terrorisme dans l'UE, par type
de terrorisme sur 2019-2021



Source : Europol, Rapport sur la situation et les tendances du terrorisme dans l'UE 2022

Risques émergents de FT

1

Réseaux sociaux/financement participatif

Envoi de fonds au moyen de campagnes de financement participatif en ligne faciles d'accès et destinées à une cause réelle et concrète

Analyser

Activité du portefeuille en ligne

Clients - Recherche dans les médias

2

Monnaies virtuelles

L'utilisation de devises numériques, de cryptomonnaies et de prestataire de services d'actifs virtuels (PSAV) permet aux groupes terroristes et extrémistes d'abuser de plus en plus des activités de financement participatif, tout en maintenant un niveau d'anonymat plus élevé pour les donateurs et les bénéficiaires

Analyser

Activité virtuelle en termes de clients et de transactions Clients de PSAV

3

OBNL

Par le passé, des organisations terroristes ont utilisé les OBNL comme des intermédiaires du FT ou pour dissimuler des détournements clandestins de fonds à des fins terroristes.

Analyser

Activité des OBNL, OBNL opérant dans les régions frontalières proches des juridictions à risque en matière de FT.

Financement du terrorisme – Exemples

- **Ali Shukri Amin**, condamné à 11 ans de prison à perpétuité pour soutien à l'EIIL (Daesh). Il a admis avoir utilisé Twitter pour fournir des conseils et des encouragements à l'EIIL et à ses partisans. M. Amin, qui utilisait le pseudonyme Twitter @Amreekiwitness, donnait des instructions sur la manière d'utiliser le bitcoin, une monnaie virtuelle, pour masquer la fourniture de fonds à l'EIIL, ainsi que pour faciliter la tâche des partisans de l'EIIL qui cherchaient à se rendre en Syrie pour combattre aux côtés de l'EIIL. Plus de 4 000 personnes se sont abonnées au compte Twitter de M. Amin, qui a servi de plateforme pro-EIIL en diffusant plus de 7 000 tweets.
- **Financement participatif –** Le 4 février 2022, GoFundMe a clôturé une campagne de soutien au **« Convoi de la liberté »** (*Freedom Convoy)* par crainte qu'elle ne soit devenue une « occupation » et à la suite de nombreux signalements faisant état de violences. Le financement participatif a également soutenu **des agents opérationnels de l'État islamique (EI)** en Syrie. Au total, la page de financement participatif a permis de collecter 10 millions de dollars.

Risque émergent – Signaux d'alerte liés aux AV

Transfert d'un grand volume d'AV vers plusieurs PSAV étrangers dans des juridictions à haut risque

Transactions entrantes provenant de nombreux portefeuilles et portant sur des montants relativement faibles

Entités opérant en tant que PSAV non enregistré/non licencié sur des sites d'échange peer-to-peer.

Recevoir des fonds de PSAV ou envoyer des fonds à des PSAV mal connus (diligence raisonnable et connaissance client) et qui ne sont pas soumis à la supervision LCB/FT

Risque émergent – Signaux d'alerte liés aux OBNL

Utilisation fréquente d'argent liquide

Dons pour les frères/la lutte/et autres termes connexes

Ambiguïté quant à l'objectif de l'OBNL ou incohérences entre l'objectif et les activités réelles

Structures financières et opérationnelles inutilement complexes au sein des OBNL, entraînant un manque de transparence quant à l'origine et/ou l'utilisation des fonds

Risques émergents de FT – Financement du Hamas

- Le 18 octobre, l'OFAC a désigné des opérateurs du Hamas et des facilitateurs financiers
- Facilitateur financier basé au Qatar qui gère les actifs secrets du portefeuille d'investissement du Hamas et entretient des liens étroits avec l'Iran, un commandant clé du Hamas et un bureau de change de devises virtuelles basé à Gaza.
- Outre les fonds que le Hamas reçoit de l'Iran, son portefeuille mondial d'investissements génère des sommes considérables grâce à ses actifs, estimés à des centaines de millions de dollars, auprès de sociétés opérant au Soudan, en Algérie, en Turquie, aux Émirats arabes unis et dans d'autres pays.
- Les entreprises du portefeuille du Hamas ont opéré sous le couvert d'entreprises légitimes et leurs représentants ont tenté de dissimuler le contrôle exercé sur leurs actifs par le Hamas.
- Le bureau d'investissement du Hamas détenait des actifs d'une valeur estimée à plus de 500 millions de dollars, notamment des sociétés opérant au Soudan, en Turquie, en Arabie saoudite, en Algérie et aux Émirats arabes unis.

Financement du Hamas – Alerte FinCen

- Un client réalise des transactions avec une entreprise de services monétaires (ESM) ou autre institution financière, y compris offrant des services en monnaie virtuelle et opérant dans des juridictions à haut risque liées à l'activité du Hamas, dont on peut raisonnablement penser ou soupçonner que les procédures de vigilance à l'égard de la clientèle sont laxistes, que sa structure de détention est opaque, ou qu'il ne respecte pas les bonnes pratiques de LCB/FT.
- Un client réalise des transactions avec des entités qui sont des sociétés-écrans, des « sociétés de négoce » ou d'autres sociétés qui ont un lien avec l'Iran ou d'autres groupes terroristes soutenus par l'Iran, tels que le Hezbollah et le Jihad islamique palestinien, ou des transactions qui sont dirigées vers ces entités ou les impliquent d'une autre manière.
- Un client qui est une organisation caritative ou un organisme à but non lucratif (OBNL) sollicite des dons mais ne semble pas fournir de services caritatifs ou soutient ouvertement l'activité ou les opérations terroristes du Hamas. Dans certains cas, ces organisations peuvent publier des messages sur des plateformes de réseaux sociaux ou des applications de messagerie chiffrées pour solliciter des dons, y compris en monnaie virtuelle.
- Un client qui est une organisation caritative ou un OBNL reçoit des dons importants d'une source inconnue sur une courte période et envoie ensuite des virements électroniques ou des chèques importants à d'autres organisations caritatives ou OBNL.

Risques émergents – Ce que nous faisons en pratique.

Que doivent faire les IF et les EPNFD face aux risques émergents ?

RISQUES ÉMERGENTS

ÉTAPE 1 — **IDENTIFIER LES RISQUES ÉMERGENTS**

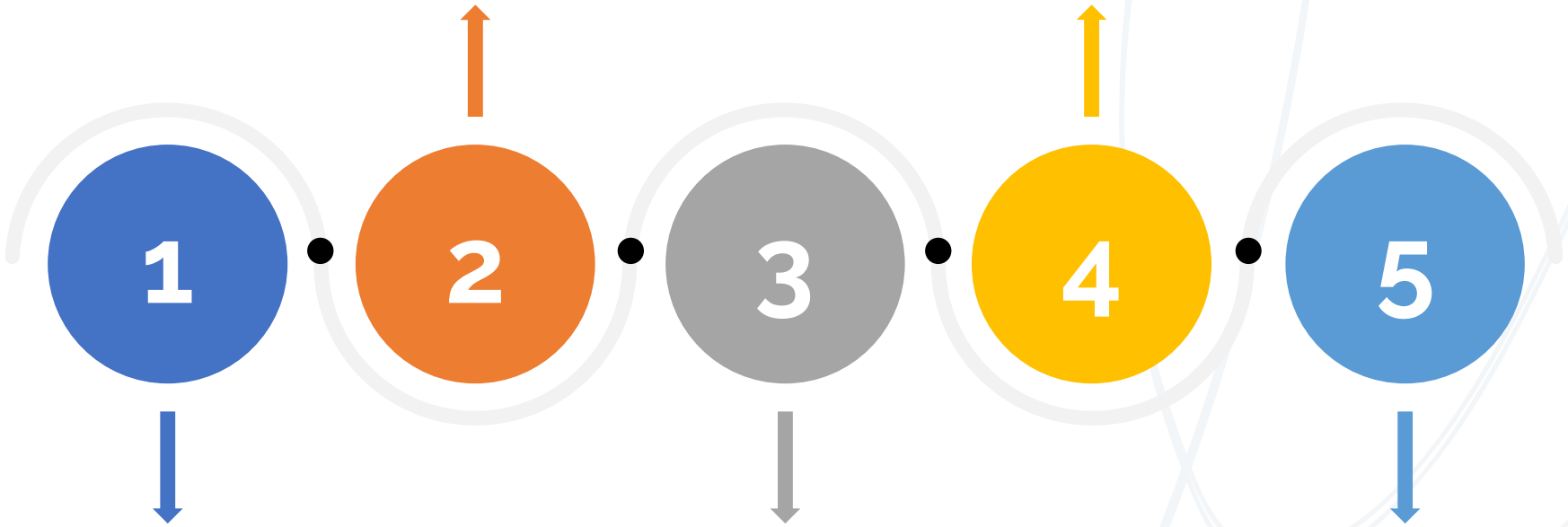
ÉTAPE 2 — **ANALYSER LES RISQUES PAR L'ÉVALUATION DE L'INSTITUTION/DE L'ENTREPRISE**

ÉTAPE 3 — **CONCEVOIR UNE RÉPONSE AU RISQUE**

ÉTAPE 4 — **METTRE EN ŒUVRE DES CONTRÔLES D'ATTÉNUATION**

RISQUES ÉMERGENTS

Comment identifier les risques émergents



ANALYSE D'HORIZON

Publications de l'UE

Publications d'autres juridictions

GAFI

ÉVALUATION DES RISQUES DE L'ENTREPRISE (ERE)

Tendances et développements identifiés

ENR/ESR

Risques identifiés et traités dans l'ENR/ESR

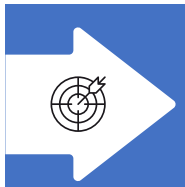
SURVEILLANCE DES OPÉRATIONS

Nouveaux modèles basés sur les transactions des clients

ANALYSES GLOBALES

Tendances et modèles basés sur l'analyse de données plus génériques

Réponse aux risques

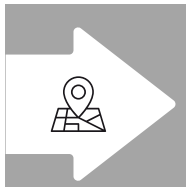


Revue de l'ERE

Sur la base des risques émergents identifiés dans l'ERE

Revue de l'ERC

Est-il nécessaire d'adapter la méthodologie et d'introduire de nouveaux facteurs de risque ?



Revue des transactions et des clients

Sélectionner les profils des clients

Sélectionner les transactions en fonction des risques

Revue des contrôles existants

Des contrôles sont-ils en place pour faire face aux risques émergents ?

Réponse aux risques

Analyses périodiques des flux de fonds (virements électroniques/transferts de fonds/P2P) à destination et en provenance de juridictions à haut risque, en vérifiant le profil et l'activité des clients

Opérations en espèces effectuées par des résidents de juridictions à haut risque

Transactions en monnaies virtuelles – identifier les clients qui effectuent un grand nombre d'opérations Correspondance entre les transactions en monnaie virtuelle et le suivi des transferts de fonds sortants

Plateforme en ligne de surveillance des commerçants – Opérations en cartes

Analyses de la clientèle dans le secteur du commerce (juridictions des transferts de fonds, comparaison avec les périodes précédentes)

Revue des OBNL et organisations caritatives – si vous disposez d'informations à jour sur les activités, celles-ci sont-elles conformes au profil ?

Réévaluation des structures d'entreprise complexes

Revue de tous les clients ayant une activité de financement participatif

Mise en œuvre de contrôles d'atténuation

Appétence pour le risque

Révision à la hausse ou à la baisse

Renforcer les contrôles informatiques

Introduire de nouveaux scénarios de surveillance des opérations

Introduire de nouveaux contrôles en temps réel

Renforcer les processus

Accroître la vigilance clientèle/renforcée

Renforcer l'examen périodique

FINANCIAL TRANSPARENCY ADVISORS

Merci pour votre temps

Financial Transparency Advisors GmbH
Zieglergasse 38/7/1070 Vienna, Austria

Phone: +43 1 890 8717 11

www.ft-advisors.com

http://www.ft-advisors.com

Prochaine session :

19/12/2023

Sujet :

Processus de suivi de Monaco avec le GAFI

Organisateur du jour : Jan Bellenghi

Présentateur du jour : Tamar Goderdzishvili