Supranational risk assessment on money laundering and terrorist financing (SNRA)

DG Justice and Consumers - B3 Financial crime Kallina SIMEONOFF



a



Action plan TF - two strands of actions

Action Plan on TF published on 2 February 2016



In a nutshell

The SNRA is a <u>tool</u> of the Commission which is required <u>under EU law</u> to



Why a supranational risk assessment?

FATF recommendations and 4th AML Directive





What is a supranational risk assessment in the EU context?

Legal mandate of 4th AML Directive





Article 6 of Directive (EU) 849/2015

- Scope: the risk assessment covers at least:
 - areas that are at greatest risks;
 - risks associated with each relevant sector:
 - most widespread means used by criminals,
 - Specifically address gambling (article 2.1 (f))
- Risk assessment published within 2 years after the adoption of the Directive (June 2017). Update every 2 years.
- Support from:
 - European Supervisory Authorities (ESAS) (joint opinion)
 - Involvement of MS experts in AML/CFT, FIUs representatives and other competent EU bodies (Europol, ESAs).



Scoping of the SNRA:

- Scope in: scope in line with the legal basis
- 2 Phases:



Scoping sectors covered

Sectors covered by 4AMLD:

- (1) credit institutions;
- (2) financial institutions;
- (3) the following natural or legal persons:
- (a) auditors, external accountants and tax advisors;
- (b) notaries and other independent legal professionals, when they participate in certain activities;
- (c) trust or company service providers;
- (d) estate agents;
- (e) traders in goods (payment in cash >EUR 10 000);
- (f) providers of gambling services;

Other Sectors/products at risk not yet included in 4AMLD (e.g. virtual currencies, crowdfunding, cash, gold, NPOs)



What is a "risk"?

A risk = the ability of a threat to exploit a vulnerability of a sector

E.g.: ability of organised crime to launder proceeds of drug trafficking by using deposit accounts in credit and financial institutions.

E.g.: ability of terrorists to collect and transfer funds by using virtual currencies

E.g.: ability of terrorists to collect funds through consumer credit by using

How to measure?



Threat: intent + capability

Vulnerability:

- 1. Inherent risk exposure
 - **Product**: speediness or anonymity of transactions, delivery channels, volume of transactions, cash involvement, management of new technologies/payment methods
 - Customer: high-risk customers, management of BO risks
 - Geographical risk: high-risk areas, size of CB transactions
- 2. Awareness of the risk/vulnerability
 - Awareness by the sector; organisational framework
 - Awareness by competent authorities; LEA capacity to counter ML/TF
 - FIU detection and analysis
- 3. Legal framew stT>> BDCgal frame5(e)3(56-ontro)5(y)]s



Methodology: 5 steps

STEP 1: identification of the risks

STEP 2: assessment of the threats

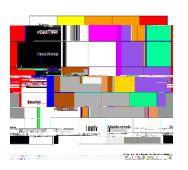
STEP 3: assessment of the vulnerabilities

STEP 4: Combination to identify the level of risks

STEP 5: Identification of mitigating measures



Specific workstream for TF





Output - deliverables

COM report (including mitigating actions such as new policy initiatives and recommendations to MS)

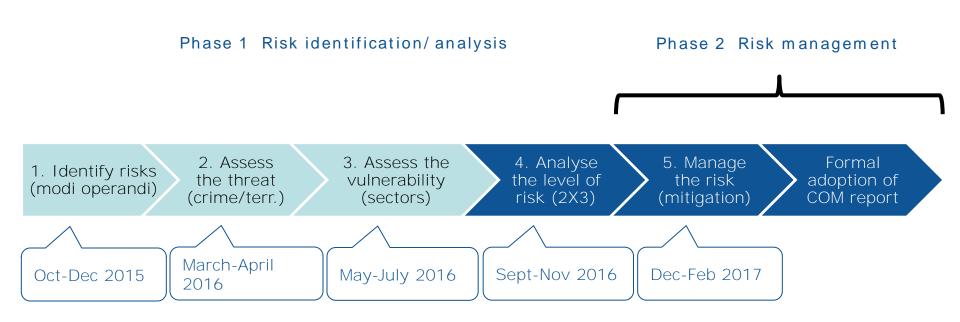
Staff Working Document ("public SNRA")

In case of need, confidential part (confidential annexes)





Process overview





Known risks:

Banking/ credit sector, MVTS, prepaid





Thank you for your attention

Contact: kallina.simeonoff@ec.europa.eu

