Supra-National Risk Assessment

November 2018

DG Justice and Consumers – Unit Financial crime
Pedro Burgos

Justice

Index

- Definition & Aims
- Legal framework: SNRA, NRA, OEs RBA, Supervision, Statistics
- Methodology
  - Scoping of the SNRA
  - Risks
  - Vulnerabilities
  - Process overview
  - Fiches
- Financial sector – Non Financial sector
- Horizontal vulnerabilities
- Mitigating meassures

In a nutshell…

The SNRA is a tool of the Commission which is required under EU law to understand risks and elaborate policies with a view to address risks of money laundering and terrorist financing.

Aim:

* Understand
* Assess
* Mitigate

ML&FT risks in EU

Why a supranational risk assessment?

FATF recommendations and 4th AML Directive

European Commission

What is a supranational risk assessment in the EU context?

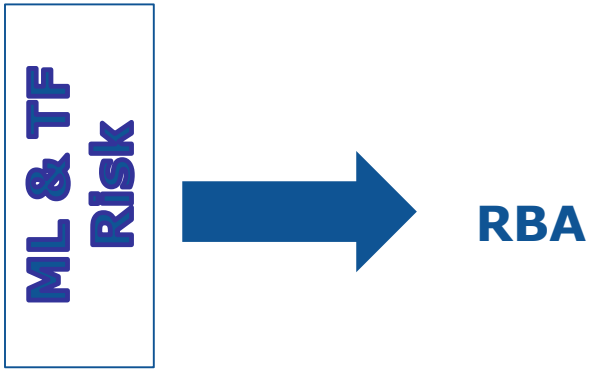
Legal mandate of 4th AML Directive

Legal framework. 4th AMLD (1)

Recitals:

- **(22)**
  - Different ML & TF risk → Holistic RBA
  - Use of evidence-based decision-making

- **(23)**
  - Identify
  - Understand
  - Mitigate



  - ESAs opinion (Joint Comitee)

Legal framework. 4th AMLD (2)

Recitals:

- **(24) COM**
  - Cross-border threats affecting internal market
  - Assessment coordinated by the European Commission
    - ✓ EGMLTF, FIUs, Union-level bodies
    - ✓ NRAs
- **(25)**
  - Risk assessments available to OE
- **(26)**
  - NRA available to mitigate risks at Union level (COM & ESAs)

Legal framework. SNRA

- **Art. 6**
  - **COM** Risk AM&TF → Internal market & XB activities
    - June 2017 SNRA Report
  - SCOPE
    - ✓ Great Risk Areas of the internal market
    - ✓ Risk associated to each relevant sector
    - ✓ Most widespread means to launder money
  - COM → SNRA available to MS & OE
  - COM → Recommendations to MS
  - ESAs → Opinion (JC) on ML&TF risks affecting financial sector. (2 years)
  - New SNRA every 2 year

Legal framework. NRAs

- **Art. 7**
  - **MS** → **Identify, asses, understand & mitigate ML&TF Risks**
  - National authority to coordinate NRA
  - Aims:
    - ✓ Improve AML/CFT regime. Enhanced Measures by OEs
    - ✓ Prioritize resources to combat ML & TF
    - ✓ Appropriate rules
    - ✓ Information for OEs Risk Assessments
  - Available to COM, ESAs & MS

Legal framework. OEs RA

- **Art. 8**
  - **OEs** Risk AM&TF.
    - Customers, countries, geographic areas, products, services,….
    - Proportioned to the OE nature & size
  - Documented, kept up-to-date & available to competent authorities
  - OEs have to put in place policies, controls, and procedures to mitigate Risks. (proportionate)
  - Policies, controls, and procedures:
    - Model risk management practices, CDD, reporting, record-keeping…
    - Independent audit function

Legal framework. Supervision

- **Competent authorities shall apply RBA to supervision (Art. 48.6)**
  - Clear understanding of ML&TF risk in MS
  - Have on-site & off-site access to relevant information
  - Intensity of inspections based on the risk profile of OE
- **Take into account the degree of discretion of the OEs to elaborate their risk assessments**
- **Self-regulatory bodies role**
- **ESAs Guidelines on RBA to supervision**

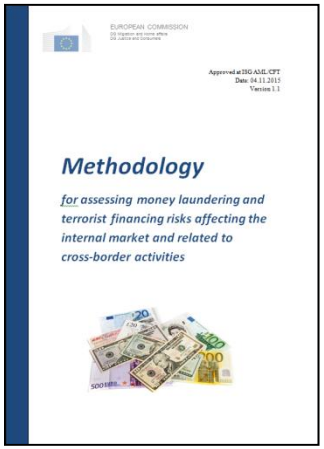
Legal framework. Statistics

- **MS - Comprehensive Statistics to review the effectiveness of their systems. Art. 44.1**
- **Type of Statistics. Art 44.2**
  - To measure the size and importance of every sector
  - To measure the reporting, investigation & judicial phases of each national AML/CFT regime
  - Number & % of reports resulting in further investigations. Annual report
  - XB request
- **Publish & transmit to COM**

European Commission

How to conduct a supranational risk assessment in the EU context?

SNRA Methodology



Justice

SNRA methodology and project charter

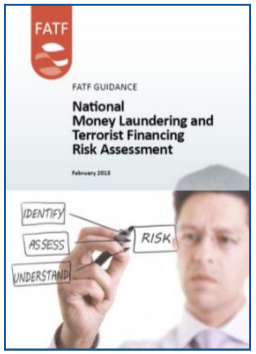
➔ Need for common understanding + FATF INR1

➔ Approach chosen: tailor-made methodology

➔ **Objectives:**

- definition of methodological guidelines,
- governance,
- working arrangements and road map,
- interaction with relevant stakeholders.

➔ based on EC methodology for security related risk assessment (DG HOME)



Methodology: 5 steps

STEP 1: identification of the risks

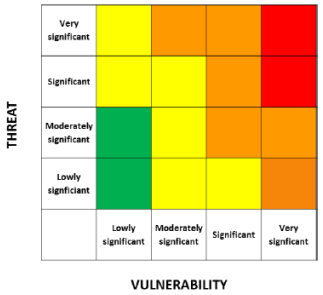
STEP 2: assessment of the threats

STEP 3: assessment of the vulnerabilities

STEP 4: Combination to identify the level of risks

STEP 5: Identification of mitigating measures

⇨ **Specific workstreams for ML+TF**



Scoping of the SNRA:

- **Scope in**: scope in line with the legal basis
- 2 Phases:
  - **1) Risk identification and analysis (MS/Agencies/DGs)**
  - **2) Risk management (COM)**
- Substantial issue:
  - **Need to cover existing and emerging risks**
  - **Focus on "supranational risks" affecting the internal market**
  - **Use of information sources (reports, NRA, intel)**
  - **Quantitative and qualitative information**
  - **Scope out: it is not a mere compilation of NRAs**

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

- Ex: ability of organised crime to launder proceeds of drug trafficking by using deposit accounts in credit and financial institutions.
- Ex: ability of terrorists to collect and transfer funds by using virtual currencies
- Ex: ability of terrorists to collect funds through consumer credit by using forged documents

How to measure the vulnerability?

1. Inherent risk exposure
   - **Product:** speediness/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 cross-border 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 framework and controls in place
   - Existing **legal framework**
   - **Effectiveness of controls** in place by entities: CDD, internal controls, STR reporting
   - Domestic and international **cooperation** between AML authorities

Consultation process

- Series of SNRA Workshops with dedicated workstream ML + TF
- Involving Member States, EU Agencies and COM (**Regulators, LEA, FIUs, Supervisors, Intel/EU Incent)**
- Expert Group (EGMLTF)/EU FIU platform to be consulted on the results

Private sector involvement

Meeting with private sector stakeholders

- **financial sector**
- **legal professionals and other DNFBPs**
- **Gambling**
- **NGOs/academics**

Process overview (Ongoing SNRA)

Phase 1–Risk identification/analysis

Phase 2–Risk management

1. Follow up recommendations	2. Update Risks & Assess emerging risks	3. Assess the vulnerability (sectors)	4. Analyse the level of risk (2X3)	5. Manage the risk (mitigation)	Formal adoption of COM report
Apr-Sep 2018	Sep-Oct 2018	Nov-Dec 2018	Dec-Jan 2018	Jan-March 2019	June 2019

CONSULTATION

CONSULTATION

Justice

Risk Matrix

			RISK MATRIX			
Threats	4	Very	2,2	2,8	3,4	4
	3	Significant	1,8	2,4	3	3,6
	2	moderately	1,4	2	2,6	3,2
	1	Lowly	1	1,6	2,2	2,8
40%			Lowly	moderately	Significant	Very
			1	2	3	4
60%			Vulnerability			

RISK LEVEL- RESIDUAL RISK	
1-1,5	LOW
1,6-2,5	MEDIUM
2,6-3,5	HIGH
3,5-4	VERY HIGH

Fiches

- **FinTech**
- **E-Money**

Financial sector

- **Moderate** level of risks due to controls/RA
- However **certain sub-sectors** more at risks (private banking, institutional investments)
- Products still at greater risk due to **anonymity features**: e-money, crowdfunding, VC, occasional transactions
- **Monitoring** in MVTS and safe deposit boxes
- Challenges posed by **Fintech**

Non-Financial sector

- High risk posed by **legal professionals/TCSPs**
  - Beneficial ownership information
  - Application of controls (legal privilege issue for LP)
  - Low reporting levels and role of self-regulatory bodies
- High risk posed by **real estate sector**
- Detailed analysis of gambling sector: online gambling, betting and poker
- Issue of **trade-based money laundering**

Horizontal vulnerabilities due to anonymity

- **Anonymous financial products**
- **Cash remains most recurring means used for ML/TF**
  - High value dealers due to weak controls
  - Cash intensive business
  - Large denominations (€500 banknotes)
  - Cash-like assets (gold, diamonds, PPC)
  - Lifestyle goods and antiquities
- **Transparency of beneficial ownership**
  - Widespread use of opaque structures
  - Use of nominee directors / senior manager

Horizontal vulnerabilities - public

- **AML supervision**
  - ➢Supervision in Home/host context
  - ➢Information exchange between supervisors
  - ➢Risk understanding and effectiveness

- **FIU cooperation**
  - ➢Limits in FIU domestic powers
  - ➢Information exchange at EU

Horizontal vulnerabilities - private

- **Infiltration and illegal services**
- **Information limits for effective monitoring**
  - Private/public information sharing
  - Forged documents
- **Resource and risk awareness and AML know-how by obliged entities**
- **Fintech**

Mitigating measures

- **European Commission**
  - Legislation: 4AMLD, Amending of 4AMLD (BO, VC, Pre-PC, FIUs)
  - Policy measures: cash payment, FIU, Fintech / e-Identification
  - Support measures: guidance (OT), training, supervision, statistics

- **Supervisors**
  - Raise awareness and risk understanding (sub-sectors)
  - Enhance cooperation between supervisors
  - TF on passporting regime
  - Guidance on compliance officer, BO

- **Recommendations to Member states**
  - Scope of NRA and obliged entities
  - Increased supervision and on-site visits (FI and non-FI)
  - Sectorial and thematic Guidance

Output - deliverables

- **COM report (including mitigating actions such as new policy initiatives and recommendations to MS)**
- **If necessary: Staff Working Document (public annexes)**
- **If necessary: confidential annexes (confidential part)**

European Commission

Thank you for your attention!