EUROPEAN COMMISSION
DG Migration and Home affairs
DG Justice and Consumers

Approved at ISG AML/CFT
Date: 04.11.2015
Version 1.1

Methodology

for assessing money laundering and terrorist financing risks affecting the internal market and related to cross-border activities

A risk means the ability of a threat to exploit the vulnerability of a sector for the purpose of money laundering or terrorist financing. A risk falls within the scope of this assessment as soon as it affects the internal market because of its characteristics – whatever the number of MS concerned (i.e. even if it may concern only one Member State). The scope covers both known and emerging risks – i.e. whether the risk materialised or not.

1. INTRODUCTION

The Financial Action Task Force (FATF) recommends that countries shall consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of each sector submitted to AML/CFT requirements when they decide to conduct a risk assessment. Money laundering (ML) and terrorist financing (TF) risks shall be identified, assessed and understood, and measures to prevent ML/TF shall be commensurate with the risks identified.

On the basis of these recommendations, the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[1] recognises the importance of a supranational approach to risk identification. It tasks the Commission to conduct the review of specific risks that could arise at European level and could affect the internal market ("supranational risk"). The Commission shall therefore conduct such Supranational Risk Assessment on money laundering and terrorist financing ("SNRA"). A risk identification is also conducted at national level by each Member States so that to ensure proper risk identification and risk mitigation of national specific risks. A third layer of risk identification is provided by sectors themselves, taking into account risk factors including those relating to their customers, countries, products, services, transactions or delivery channels.

These three layers of risk assessments (and where appropriate risk mitigation) allow building a comprehensive awareness and analysis of ML/TF risks in the European Union. There are complementary and have the same level of relevance as regards, respectively, the sectorial, national and supranational approach to the risk assessment.

Even though national and sectorial risk assessments, among other sources, may prove to be essential building blocks for the SNRA conducted by the Commission, it cannot be considered as a mere compilation of these ones. The SNRA exercise shall therefore be

[1] O.J. L.141, 5.06.2015, p.73

understood as a separate work stream. This is a pre-requisite for an efficient exercise consistent with the mandate of the Directive (EU) 2015/849, especially when the Commission will make recommendations to Member States on the measures suitable for addressing the identified European ML/TF risks. In carrying out the national risk assessments, Member States shall also make use of the findings of the SNRA report.

2. SCOPE AND OBJECTIVE

The aim of this document is to define methodological guidelines, governance, working arrangements and road map in order to support the conduct of the risk assessment and the interactions with relevant stakeholders in terms of inputs, expertise and advice.

The objective and scope of the risk assessment is defined in article 6 of Directive (EU) 2015/849 (see annex 3 for the provisions of the Directive). For the purpose of this methodology, the objective is to carry out an **assessment of supranational ML/TF risks** (see annex 4 for the definitions).

The "evaluation" of the identified and assessed risks (outcomes of the risk assessment) is out of the scope of these methodological guidelines and shall be considered within the framework of the overall risk management process leading to the identification of mitigation measures to fill the identified residual risks (see annex 2).

3. ROLES AND RESPONSIBILITIES ON EU SUPRANATIONAL RISK ASSESSMENT

3.1. ROLE OF THE COMMISSION

Following the mandate given by Article 6 of the Directive (EU) 2015/849, the Commission is responsible for drawing up the SNRA report and for defining the mitigating measures.

The Commission will conduct the assessment by:
- organising the work at European level and involving the appropriate experts;
- making the joint opinions of the European Supervisory Authorities (ESAs) as well as the SNRA report available to the Member States and obliged entities;
- defining the mitigating measures, making recommendations to Member States on the measures suitable for addressing the identified risks.

In that context, though the Commission will rely on the expertise of several stakeholders (see point 3.3), **it will have a decisional power to validate the outcomes of the SNRA discussions**.

An Inter-service Group of the Commission will act as steering group for this exercise.

3.2. ROLE OF THE AD HOC WORKING GROUP

In order to define a risk assessment methodology, an Ad Hoc Working Group (ADHWG) composed by volunteers from Member States has been set up in February 2014. The role of the ADHWG is to support the development of the methodology for carrying out the identification, assessment and evaluation of the supranational ML/TF risks as provided for in the Directive (EU) 2015/849. The ADHWG will follow the approach defined by FATF in its "Guidance on National Money Laundering and Terrorist Financing Risk Assessment"

published on February 2013[2]. Following the finalisation of the methodology, the ADHWG will be consulted on methodological implementation issues and changes in case of need.

3.3. ROLE OF OTHER STAKEHOLDERS

During each step of the process, the Commission will involve the relevant experts from Member States[3] and European bodies as defined in the Directive. Where appropriate, the Commission will also involve representatives from the private sector, NGOs or academics in the process. Input and relevant information could be requested to the following stakeholders through ad hoc processes (public consultation, questionnaires, preparation of background papers, bilateral meetings…):

Experts group on money laundering and terrorist financing (EGMLTF): EGMLTF is a permanent Commission expert group composed of national administrations with the mandate of assisting the Commission, e.g. in the preparation of policy definition and providing expertise to the Commission when preparing implementing measures. EGMLTF has the capacity to draw on expertise available nationally.

> => *EGMLTF may provide data relating* ***to national risk assessments and more generally information on risks, threats and vulnerabilities***. *The role of EGMLTF in regard of the SNRA is also to appoint national experts for the different workshops*.

European Supervisory Authorities (ESAs): the ESAs (European Banking Authority, European Securities and Markets Authority, European Insurance and Occupational Pensions Authority) are tasked under article 6(5) of Directive (EU) 2015/849 with the responsibility of issuing a joint opinion on the ML/TF risks **affecting the Union's financial sector**.

[2] see http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

[3] Throughout this document, indications about the composition of the Member States experts groups designated to conduct the risk identification and risk assessment are provided for sake of information. However, the appointment of the most relevant experts is left to the appreciation of each Member States by considering the specific expertise required for each dedicated phase of the risk identification and assessment. It may include representatives of supervisory authorities, financial intelligence units, customs, gambling sectors, ministerial authorities, law enforcement, etc…

Considering the key role the ESAs play in the identification of risks related to the financial sector, they participate directly to the discussions held within the ADHWG. In addition, regular contacts are organised between the Commission services responsible to draw up the SNRA report and the working group of the ESAs in charge of the joint opinion.

=> *ESAs may provide data relating to distinctive features of ML/TF risks from a supervisory perspective, ML risks associated with the financial sectors' systems and controls, taking into account the various typical sectorial business models, strategies and cultures*..

Other financial supervisory authorities not represented by the ESAs: considering the wide range of actors responsible for financial supervision, contacts will be held with other supervisory authorities not represented in the ESAs.

EU Financial Intelligence Units (EU FIUs): FIUs cooperate at the EU level through a group called the FIU Platform which main task is to facilitate cooperation among EU FIUs. Work of the FIU Platform and the EGMLTF should be closely coordinated

=> *The FIU Platform may provide* ***data relating to national risk assessments, distinctive features of ML/TF risks from an FIU perspective (annual reports), aggregated data on suspicious transactions reports***..

Sectorial specific expert groups: the Commission manages a number of groups of Member States experts covering the different sectors exposed to the ML/TF risks. Those networks may provide useful information and data regarding their respective sectors.

=> *Such experts group may be consulted especially for preparing the assessment of the sectors' vulnerability*.

Europol: Europol is an EU agency which supports law enforcement authorities by gathering, analysing and disseminating information.

=> *Europol may provide data relating to organised crime threat assessments (e.g. "organised crime threat assessment report" which includes analysis on money laundering threats). It may also provide analyses and intelligence work on AML/CFT from a law enforcement perspective*.

Eurostat: Eurostat is a Directorate General of the European Commission which provides statistics at European level that enable comparisons between countries and regions.

=> Eurostat may provide data relating to series of indicators for the different stages of the AML chain, from the filing of a suspicious transaction report through to conviction (ML report 2013). It may also provide statistical data on economy, sectors and products.

Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRB): FATF is an inter-governmental body which sets standards and promotes effective implementation of legal, regulatory and operational measures for combating ML, TF and other related threats to the integrity of the international financial system. FSRBs have been established for the purpose of disseminating FATF Recommendations throughout the world. The main task of the FSRBs is to devise systems for combating ML/TF risks in their respective regions.

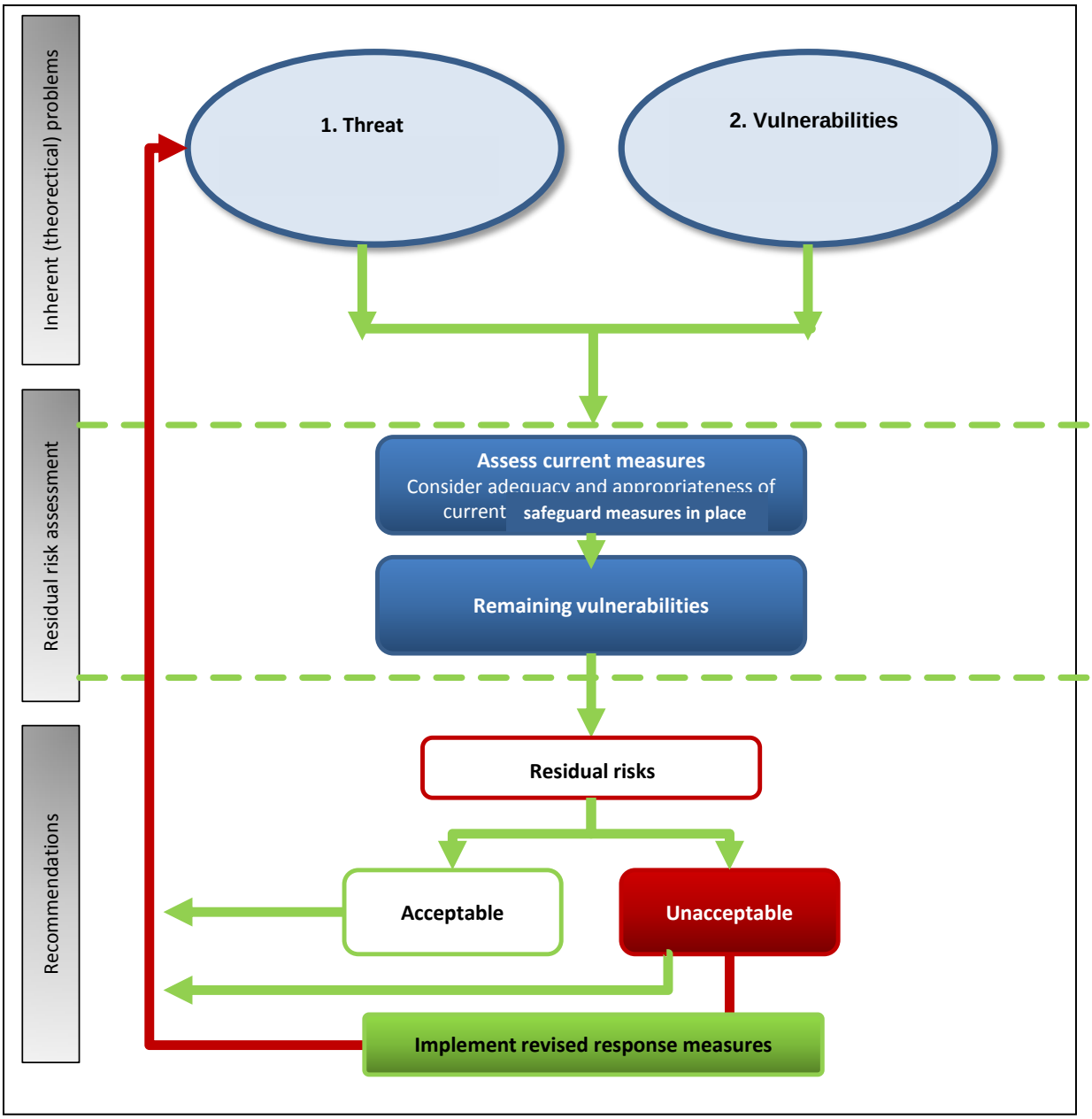
=> The FATF and FSRBs conduct evaluations of the AML/CFT systems of the Member States and are developing studies of typologies – the most common schemes used by criminals for ML/TF-that will provide useful information to feed the SNRA.

Other relevant stakeholders such as Non-Governmental Organisations (NGOs), private sector representative bodies at European level (DNBPs, financial sectors etc.) and other public or private sector organisations may also provide useful information.

4. METHODOLOGICAL APPROACH

4.1 RISK MANAGEMENT FRAMWORK

The conceptual framework for this methodology can be summarised as follows:



4.1.1 METHODOLOGICAL APPROACH

Because of their specific features, FT and ML risks will be considered and assessed within two separate work streams.

The proposed methodology is based on the following consecutive actions:

1. The identification of ML and TF mechanisms (*modi operandi*) that could constitute ML/TF risks at EU level. There are intended as ML/TF mechanisms going beyond the specificities of national jurisdictions, whatever they arise in one or several Member States and which may represent a risk from an internal market perspective.

2. An assessment of the level and nature of threats related to estimated intent and capability to exploit mechanisms for ML and TF, i.e. a clear *modi operandi* approach by "sector" (scenario based approach), in all sectors mentioned in article 2 and 4 of the Directive (EU) 2015/849. In this specific application, the assessment focuses on the estimated intent and capability of criminals to exploit existing or innovative mechanisms for ML and TF. The assessment will be based on Member States' experts and other relevant stakeholders estimates, conducted on the basis of available intelligence, information (qualitative and quantitative inputs) and in light of the agreed approach to threat assessment (clearing house threat assessment reconciliation method). The Commission, which will have a decisional power to validate the outcomes of the SNRA discussions, will assess the strategic level of threat to be respectively:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

3. An assessment of the level and nature of vulnerabilities by sector to ML/TF exploitable mechanisms (*modi operandi*). The vulnerability assessment will focus on the assessment of

existing safeguards in place. Based on Member States' experts and other relevant stakeholders estimates, conducted on the basis of available information (qualitative and quantitative inputs) and in light of the agreed approach to vulnerability assessment (clearing house vulnerability assessment reconciliation method), the Commission, which will have a decisional power to validate the outcomes of the SNRA discussions, will assess the strategic level of vulnerability to be respectively:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

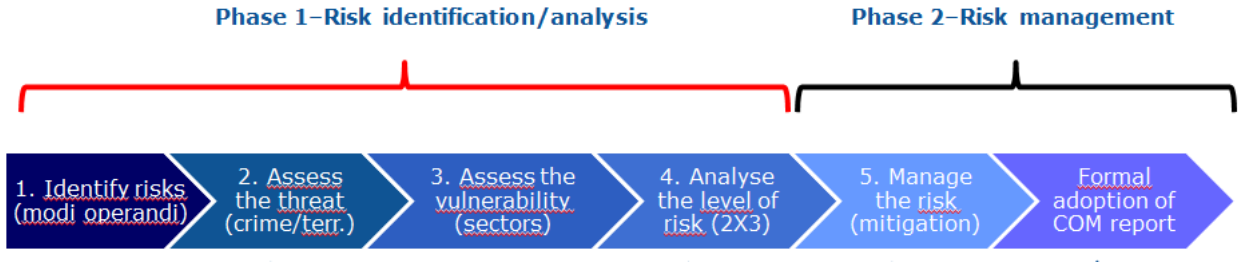
4. Determination of the residual risk on the basis of interplay of estimated threats and vulnerabilities for each type of modus operandi. The risk assessment will be built on a risk based assessment by sector. For each sector considered a set of pre-defined *modi operandi* (ML/TF exploitable mechanisms) will be assessed in terms of risk as combination of the identified level of threat and vulnerability.

For the purpose of this risk assessment the "impact/consequences" component is regarded as constantly significant and will therefore not be assessed. The proposed methodology consequently only looks at the threats and vulnerability components. While it is important to understand the consequences associated with the ML/TF activities (physical, social, environmental, economic and structural consequences), from a methodological point of view it is particularly challenging to measure their consequences in quantifiable or numerical terms. **For the purpose of this risk assessment it is therefore assumed that ML/TF activities generate constant significant negative effects** on the transparency, good governance and the accountability of public and private EU institutions, cause significant damage to EU countries national security and have both direct and indirect impact on the EU economy. From a methodological point of view, as the impact/consequences component is assumed as a fix

high value for the specific purpose of this risk assessment, the determination of the residual risk for each scenario (modus operandi versus scenario) will be determined by the combination of the identified level of threat and vulnerability.

5. PROCESS DESCRIPTION

The process can be summarised by the following steps:



A detailed roadmap is provided for the risk identification/analysis phase in Annex 1. This roadmap foresees the following consecutive actions:

5.1. STEP 1: RISK IDENTIFICATION

The first step consists in identifying the exact scope in terms of ML/TF risks to be assessed at a later stage of the risk assessment process. For the specific purpose of the SNRA as defined in Directive (EU) 2015/849, risks identification should be intended as defining a list of **known or suspected** ML/TF threats along with the related sectors exploited by criminals to successfully perpetrate ML and/or TF activities. The risk of ML and TF is not the same in every case. Accordingly, a holistic risk-based approach should be used. While the risks identification process will rely largely on known threats, it is important to give due consideration to innovative or emerging threats for which it is reasonable to assume a lack of consolidated safeguards in place. At this stage, the objective is to identify the nature of the risks scenarios (*threats versus exploitable sectors*) and those which are the most relevant considering the scope of the risk assessment. It does not seek to assess the level of these risks (significant or non-significant) which will be the objective at a later stage (estimated level of threats and vulnerabilities determining the residual risk).

5.2. STEP 2: THREAT component

This second step consists in assessing the level of threat (lowly significant (1), moderately significant (2), significant (3), very significant (4)) for each of the *scenario* (ML and TF processes *versus* exploitable sector) identified in step 1[4]. The assessment will be based on the estimated combined assessment of intent and capability of criminals to change or transfer illegitimate or legitimate funds. The assessment of the threat level for each identified risk should lead to a threat assessment level common to the EU as a whole. At this regard, it is suggested the strategic level of threat for each risk will be assessed according to the threat assessment clearing house reconciliation method.

The Commission will validate the outcomes of the threat assessment clearing house reconciliation method[5].

The "Intent" component of the threat will rely on known intent (concrete occurrence of the threat[6]) successful or foiled, and the perceived attractiveness of ML/TF through a specific mechanism. While the broad intent to ML/TF is assessed as being constantly high, intent to use specific modus operandi differs depending of the attractiveness of the ML/TF modus operandi, and the known existence of AML/CFT safeguards.

The risk assessment will therefore consider, on a scenario by scenario basis, the level of intent to exploit (IT) ML/TF mechanisms.

[4] Both the threat and vulnerability assessment are built around a four scale rating. Different rating can be considered but this latter presents the advantage (compared to a three or two scale rating) to capture better qualitative differences between the different risks. The resulting risk level is also based on a four scale rating.

[5] The clearing house reconciliation method has proven its efficacy in the framework of several EU risk assessments in the field of aviation security. For those risk assessments requiring a common EU position, which is the case for the supranational FT/ML risk assessment, the clearing house reconciliation method has proved its efficacy in providing the necessary working arrangements facilitating the achievement of a common position.

[6] It measures the concrete occurrence of the threat on the territory. The data used originate from the evidence available on the subject of reports to the particular offence or class of offences.

The "capability" component of the threat is understood as the capability of criminals to successfully change or transfer the ML proceeds of crime and to successfully transfer illegitimate or legitimate funds to financially maintaining a terrorist network.

The assessment of the capability component will consider the ease of using a specific ML/TF modus operandi for (technical expertise and support required), the accessibility and relative costs (financial capacity) of using a specific modus operandi.

5.3. STEP 3: VULNERABILITY

This third step consists in assessing the level of vulnerability (lowly significant (1), moderately significant (2), significant (3), very significant (4)) for each of the scenario (ML and TF processes versus exploitable sector) identified in step 1.

For each of the scenario identified in step 1, the vulnerability assessment **will focus on the existence and effectiveness of safeguards in place**. The more effective safeguards in place, the lower vulnerabilities and risk are.

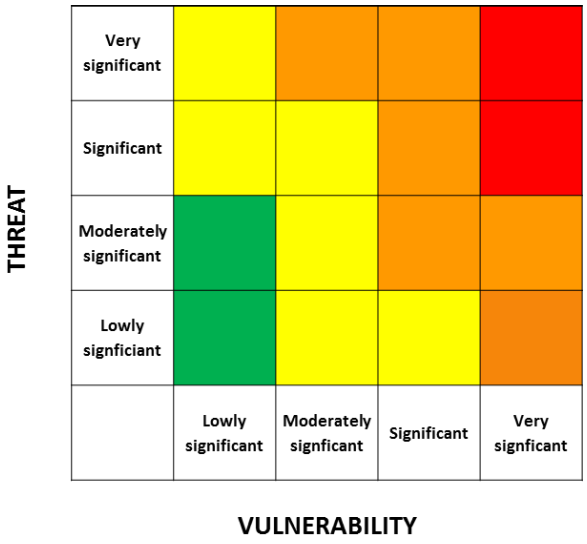
The vulnerability assessment will be performed for the areas/sectors, related to the modus operandi identified in step 1, required to implement the AML/CFT legislation.

For the specific purpose and scope of the SNRA, the vulnerability assessment will consider primarily the existence of national, EU and international legislation and their effective implementation at national level. By taking into account the EU wide nature of the ML/TF risks to be considered in the SNRA, particular attention should also be paid to other criteria such as the effectiveness of information sharing among FIU, coordination with other AML authorities and international cooperation, including between AML supervisors.

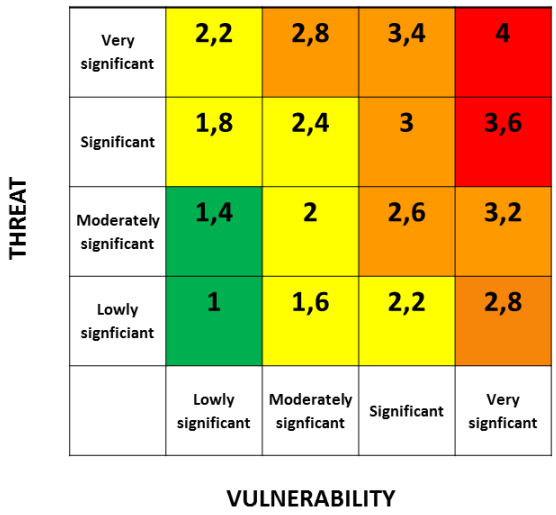
The assessment of ML/TF vulnerabilities of the system as a whole will be based on the data collected and analysed by relevant supervisory authorities, the FIU and national authorities.

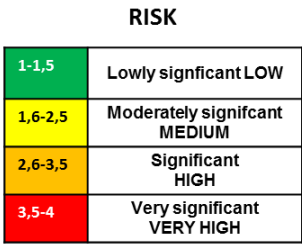
5.4. STEP 4: RESIDUAL RISK

The outcomes of steps 2A/B (threat assessment) and 3A/B (vulnerability assessment) will determine the risk level for each identified risk (steps 1A/B), as combination (matrix approach) of the assessed threat and vulnerability level.



The risk level is ultimately determined by combination between the threat *versus* vulnerability. The risk matrix determining this risk level is based on a weighting of 40 % (threat)/ 60 % (vulnerability) - assuming that the vulnerability component has more capacity in determining the risk level. It is assumed that the level of vulnerability is likely to increase the attractiveness and hence the intent of criminals/terrorists to use a given modus operandi – thus impacting ultimately the level of threat.





6. INVOLVEMENT OF PRIVATE SECTOR AND CIVIL SOCIETY

The Commission will consult the private sector and civil society during the process. It will organise dedicated workshops with the four main groups of private sector stakeholders (financial sector, legal professions, other obliged entities, Non-Governmental Organisations). The Commission will organise those workshops at two steps in the process:

- Following the risk identification: consultation on the basis of already identified risks and collection of feedback regarding the risk identification (January-February 2016)

- Following the finalization of the risk assessment: consultation on the outcome and possible mitigating actions (November 2016)

7. REASSESSMENT/EX NOVO ASSESSMENT

Based on available intelligence and information, the Commission will propose further rounds of the risk assessment to reassess the evolving threat situation or new emerging threats. The Commission ensures an updating of the risk assessment every two years, or more frequently if appropriate.

Unless there are exceptional circumstances, the first update of the SNRA would take place 2 years after the issuing of the initial SNRA report (i.e. by June 2019). This first update will be drawn up through a lighter procedure. Such lighter procedure will imply the gathering of information by written procedure (e.g. questionnaire) and will focus on the implementation of the Commission recommendations concerning the mitigating measures, and the evaluation of the risks following the mitigation.

The Commission will then assess the experience gained and, if need be, adapt its methodological approach. The second update (by 2021) would likely follow the full standard methodology for a more comprehensive assessment. It will consist of assessing the relevance of the first risk assessment outcomes by including new emerging risks.

Annex 1

Road map

Annex 1 Road Map

STEP 1/A: November 2015 – dedicated meeting: TF risks identification

Location: DG HOME secure zone

COMPOSITION: Member States experts (to be appointed by MS authorities)[7], FIU, COM (DG JUST, DG HOME), Europol, EU Intcen, ESAs

OBJECTIVE: the meeting should lead to identify TF risks (methods/modi operandi) to be considered within the risk assessment exercise according to the scope of the SNRA.

SOURCES (non-exhaustive): open sources, inputs from national risk assessment, classified threat assessment on TF issued by EU Intcen (including an update available by September 2015), inputs from Europol, TF offences listed by FAFT, intelligence from FIU.

METHODOLOGY: based on the sources above, COM will facilitate a discussion paper listing potential TF risks to be considered within the risk assessment and to be assessed a later stage (threat and vulnerability assessment). The expert group will be requested to consider their relevance in the framework of the SNRA scope and to assess whether other risks should be included.

END RESULT: define a list of TF risks (modi operandi/methods for TF) to be considered within the risk assessment.

[7] As far as the MS experts are concerned, their appointment is left to the appreciation of Member States by considering the specific expertise required for each dedicated phase of the risk assessment. For sake of efficiency, it should be ensured that the MS experts represented in the experts meetings are able to bring a position and to provide elements that has been defined and agreed at national level following a coordination process.

STEP 1/B: November 2015 – dedicated meeting: ML risks identification
Location: standard meeting room

COMPOSITION: Member States experts (to be appointed by MS authorities)[8], COM (DG JUST, DG HOME), Europol, ESAs.

OBJECTIVE: the meeting should lead to identify ML risks (methods/modi operandi) to be considered within the risk assessment exercise according to the scope of the SNRA.

SOURCES (non-exhaustive)**:** open sources, inputs from national risk assessment, available threat assessment on ML, inputs from Europol, ML offences listed by FAFT, intelligence from FIU.

METHODOLOGY: based on the sources above, COM will facilitate a discussion paper listing potential ML risks to be considered within the risk assessment and to be assessed a later stage (threat and vulnerability assessment). The expert group will be requested to consider their relevance in the framework of the SNRA scope and to assess whether other risks should be included.

END RESULT: define a list of ML risks (modi operandi/methods for ML) to be considered within the risk assessment.

[8] See footnote 3

STEP 2/A: March/April 2016 – dedicated meeting: assessing the level of threat for TF risk identified in step 1/A

Location: DG HOME secure zone

COMPOSITION: Member States experts (to be appointed by MS authorities)[9], COM (DG JUST, DG HOME), Europol, EU Intcen.

OBJECTIVE: based on the outcomes of step 1/A) the meeting should lead for each TF identified risk to assess its threat level according to a four scale approach:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

SOURCES(non-exhaustive)**:** open sources, inputs from national risk assessment, available threat assessment on financing terrorism (EU Intcen), inputs from Europol, available intelligence from Member States / FIU, inputs from financial sectors supervisors, non-financial sectors supervisors, private sector's available statistics from judicial records.

METHODOLOGY: the assessment of the threat level for each TF identified risk as resulting from step 1/A, should led to a threat assessment level common to the EU as a whole.

At this regard, it is suggested the strategic level of threat for each risk will be assessed according to the threat assessment clearing house reconciliation method.

Threat assessment clearing house reconciliation method: experts will propose an estimated level of threat for each risk identified in step 1/A. Discrepancies in threat estimates will then

[9] See footnote 3

be discussed multilateral (or bilaterally if needed), until the Commission considers that a common position, deemed as common to the EU as a whole, is agreed.

Should a difference of estimates remain –these experts will attempt to determine whether the higher threat estimate is primarily due to an estimated higher threat in a specific field or Member State rather than all EU Member States equally. If so, the level of threat which will be retained by the Commission for the purpose of the current methodology will be that which it considers as common to the EU as a whole.

The Commission will have a decisional power to validate the outcomes of the threat **assessment reconciliation method**

The "Intent" component of the threat will rely on known intent (concrete occurrence of the threat) successful or foiled, and the perceived attractiveness of TF through a specific method/mechanism. While the broad intent to TF is assessed as being constantly high, intent to use specific modus operandi/methods differs depending of the attractiveness of the modus operandi and the known existence of CFT safeguards.

The "capability" component of the threat is understood as the capability of threat groups (terrorists) to successfully transfer illegitimate or legitimate funds to financially maintaining a terrorist network.

The assessment of the capability component will consider the ease of using a specific modus operandi for TF (technical expertise and support required), the accessibility and relative costs (financial capacity) of using a specific modus operandi.

Table 1: the threat component (financing terrorism risks) will be assessed according to a four scale threat level:

LOWLY SIGNIFICANT (value: 1)	No indicators that criminals have the intention to exploit this modus operandi for ML/TF. The modus operandi is extremely difficult to access and/or may cost more than other options and perceived as unattractive and/or highly insecure. No indicators that criminals have the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires sophisticated planning, knowledge and/or high technical expertise than other options. **The threat related to the use of this modus operandi is lowly significant.**
MODERATELY SIGNIFICANT (value: 2)	Criminals may have vague intentions to exploit this modus operandi for ML/TF. The modus operandi is difficult to access and/or may cost more than other options and perceived as unattractive and/or insecure. Few indicators that criminals have some of the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires planning, knowledge and/or technical expertise than other options. **The threat related to the use of this modus operandi is moderately significant.**
SIGNIFICANT (value: 3)	Criminals have exploited this modus operandi for ML/TF. The modus operandi is accessible and/or represents a financially viable option. The modus operandi is perceived as rather attractive and/or fairly secure. Criminals have the necessary capabilities to exploit this modus operandi. The modus operandi requires moderate levels of planning, knowledge and/or technical expertise. **The threat related to the use of this modus operandi is significant.**
VERY SIGNIFICANT (value: 4)	Criminals have recurrently exploited this modus operandi for ML/TF. The modus operandi is widely accessible and available via a number of means and/or relatively low cost. The modus operandi is perceived as attractive and/or secure. Criminals are known to have the necessary capabilities. The modus operandi is relatively easy to abuse, requires little planning, knowledge and/or technical expertise required compared to other options. **The threat related to the use of this modus operandi is very significant.**

END RESULT: assessing TF threat level for each identified risk according to the 4 scale approach.

STEP 2/B March/April 2016 – dedicated meeting: assessing the level of threat for each ML risk identified in step 1/B

Location: DG HOME secure zone

COMPOSITION: Member States experts (to be appointed by MS authorities)[10], COM (DG JUST, DG HOME), Europol, EU Intcen.

OBJECTIVE: based on the outcomes of step 1/B, the meeting should lead, for each ML identified risk, to assess its threat level according to a four scale threat level:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

SOURCES (non-exhaustive)**:** open sources, inputs from national risk assessment, inputs from Commission services, inputs from Europol, available intelligence from Member States / FIU, inputs from financial sectors supervisors, non-financial sectors supervisors, private sectors, available statistics from judicial records.

METHODOLOGY: the assessment of the threat level for each identified ML risk as resulting from step 1/B, should led to a threat assessment level common to the EU as a whole. While capabilities and intent may be very different in Member States, with certain risks extremely significant in some countries and less relevant in other countries, the scope of the SNRA requires to identify a threat assessment level common to the EU as a whole.

At this regard, it is suggested the strategic level of threat for each risk will be assessed according to the threat assessment clearing house reconciliation method.

[10] See footnote 3

Threat assessment clearing house reconciliation method: experts will propose an estimated level of threat for each ML risk identified in step 1/B. Discrepancies in threat estimates will then be discussed multilateral (or bilaterally if needed), until the Commission considers that a common position, deemed as common to the EU as a whole, is agreed.

Should a difference of estimates remain – e.g. with some experts estimating threat to be "medium" and others "high" – these experts will attempt to determine whether the higher threat estimate is primarily due to an estimated higher threat in a specific field or Member State rather than all EU Member States equally. If so, the level of threat which will be retained by the Commission for the purpose of the current methodology will be that which it considers as common to the EU as a whole.

The Commission will have a decisional power to validate the outcomes of the threat **assessment reconciliation method**

The "Intent" component of the threat will rely on known intent (concrete occurrence of the threat) successful or foiled, and the perceived attractiveness of ML through a specific method/mechanism. Intent to use specific modus operandi/methods differs depending of the attractiveness of the modus operandi and the known existence of AML safeguards.

The "capability" component of the threat is understood as the capability of criminals to successfully laundering and transfer illegitimate funds.

The assessment of the capability component will consider the ease of using a specific modus operandi for ML (technical expertise and support required), the accessibility and relative costs (financial capacity) of using a specific modus operandi.

Table 2: the threat component (money laundering risks) will be assessed according to a four scale threat level:

LOWLY SIGNIFICANT (value: 1)	No indicators that criminals have the intention to exploit this modus operandi for ML/TF. The modus operandi is extremely difficult to access and/or may cost more than other options and perceived as unattractive and/or highly insecure. No indicators that criminals have the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires sophisticated planning, knowledge and/or high technical expertise than other options. **The threat related to the use of this modus operandi is lowly significant.**
MODERATELY SIGNIFICANT (value: 2)	Criminals may have vague intentions to exploit this modus operandi for ML/TF. The modus operandi is difficult to access and/or may cost more than other options and perceived as unattractive and/or insecure. Few indicators that criminals have some of the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires planning, knowledge and/or technical expertise than other options. **The threat related to the use of this modus operandi is moderately significant.**
SIGNIFICANT (value: 3)	Criminals have exploited this modus operandi for ML/TF. The modus operandi is accessible and/or represents a financially viable option. The modus operandi is perceived as rather attractive and/or fairly secure. Criminals have the necessary capabilities to exploit this modus operandi. The modus operandi requires moderate levels of planning, knowledge and/or technical expertise. **The threat related to the use of this modus operandi is significant.**
VERY SIGNIFICANT (value: 4)	Criminals have recurrently exploited this modus operandi for ML/TF. The modus operandi is widely accessible and available via a number of means and/or relatively low cost. The modus operandi is perceived as attractive and/or secure. Criminals are known to have the necessary capabilities. The modus operandi is relatively easy to abuse, requires little planning, knowledge and/or technical expertise required compared to other options. **The threat related to the use of this modus operandi is very significant.**

END RESULT: assessing threat level for each ML identified risk according to the four scale threat level.

STEP 3/A: May- July 2016 – dedicated meeting: assessing the level of vulnerability for each TF risk identified in step 2/A
Location: standard meeting room

COMPOSITION: Member States experts (to be appointed by MS authorities)[11], COM (DG JUST, DG HOME), Europol, ESAs.

OBJECTIVE: based on the outcomes of step 1/A, the meeting should led, for each identified TF risk, to assess its vulnerability level according to a four scale vulnerability level:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

SOURCES (non-exhaustive**):** open sources, inputs from national risk assessment, available threat assessment on TF (EU Intcen), inputs from Europol, available intelligence from Member States / FIU, inputs from financial sectors supervisors, non-financial sectors supervisors, private sectors, and available statistics from judicial records.

METHODOLOGY: the assessment of the vulnerability level for each identified TF risk as resulting from step 1/A, should led to a vulnerability assessment level common to the EU as a whole as result, among others, of differences between the regulatory frameworks of Member States which might induce vulnerabilities at a supra national level.

The vulnerability assessment will be performed for the areas/sectors, related to the modus operandi identified in step 1A, required to implement the TF legislation. Consideration will be also given to threats which cannot be linked to a sector.

[11] See footnote 3

For the specific purpose and scope of the SNRA, the vulnerability assessment will consider primarily the existence of national, EU and international legislation and their effective implementation at national level. By taking into account the EU wide nature of the risks to be considered in the SNRA assessment, particular attention should also be paid to other criteria such as the effectiveness of information sharing among FIU, coordination with other CFT authorities and international cooperation, including between CFT supervisors.

One of the main components of the vulnerability assessment will consider, for each category of obliged parties, the specific risk and effectiveness of CFT safeguards in place.

Table 3: the vulnerability component will be assessed according to a four scale vulnerability level:

LOWLY SIGNIFICANT (value: 1)	[Within the sector/area considered, deterrence measures and controls exist and are effective at deterring money laundering and financing terrorism. The sector shows a positive organisational framework and a negligible exposure to the risk of ML/TF]. **Illustrative assessment criteria:** **RISK EXPOSURE** - No or very limited products, services or transactions that facilitate speedy or anonymous transactions; secured and/or monitored delivery channels; low level of financial transactions; low level of cash based transactions; high quality management of new technologies and/or new payment methods - Very limited volume of higher risk customers[12]; high ability to manage corporate entities or trusts in customer relationships - No or very limited business and customer based in areas identified as high risk[13]; low level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY**

[12] A non-exhaustive list of factors and type of evidence of potentially higher risk customer is included in Annex 3 of Directive (EU) 2015/849

[13] A non-exhaustive list of factors and type of evidence of potentially higher risk countries is included in Annex 3 of Directive (EU) 2015/849. In the same text, Article 9 tasks the Commission to identify high-risk third countries

	- Sector concerned shows a satisfactory level of awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from a positive organisational framework. - Competent authorities provide a comprehensive ML/TF risk assessment related to the sector and LEAs have a high ability to counter ML/TF risks (a range of ML/TF cases is visible and highly likely to be detected, leading to investigation, prosecution and convictions) - Good ability of the FIU to detect and analyse the risks, to ensure a good functioning of gathering information through STR, in particular through the use of tailor-made indicators and a sufficient amount of resources to actually perform the risk-analysis. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework is commensurate to the risks inherent to this sector. - Controls [defined by the legislation] are effectively applied by the sector. Reliable CDD/identification mechanisms are in place to ensure adequate identification and verification process of a customer. Internal controls are applied by obliged entities in a robust manner (e.g. risk management, record keeping, training). Obliged entities are effectively reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a good level of sharing of information **=> Lowly-significant vulnerabilities.**
MODERATELY SIGNIFICANT (value: 2)	[Within the sector/area considered, deterrence measures and controls exist and are reasonably effective at deterring money laundering and financing terrorism. The sector shows an organisational framework presenting some weaknesses and/or an exposure to the risk of ML/TF.]. **Illustrative assessment criteria**: **RISK EXPOSURE** - Limited products, services and transactions that facilitate speedy or anonymous transactions; mostly secured and/or monitored delivery channels; rather significant level of financial transactions; rather significant cash based transactions; good management of new technologies and/or new payment methods - Few higher risk customers; good ability to manage corporate entities or trusts in customer relationships

	- Some business and customer are based in areas identified as high risk; rather significant level of cross-border movements of funds; **<u>AWARNESS OF THE RISK VULNERABILITY</u>** - Sector concerned shows some awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from an organisational framework which shows some weaknesses. - Competent authorities provide a reasonable ML/TF risk assessment related to the sector and LEAs have a good ability to counter ML/TF risks (a range of ML/TF cases is visible and likely to be detected, leading to some investigations, prosecutions and convictions - FIU can detect and analyse the risks in certain circumstances, to ensure a good functioning of gathering information through STR, in particular through the use of tailor-made indicators **<u>LEGAL FRAMEWORK AND CONTROLS</u>** - The existing legal framework covers in major parts the risks inherent to this sector - Controls [defined by the legislation] are applied by the sector but presenting some weaknesses. Reliable CDD/identification mechanisms are in place but do not ensure systematically an adequate identification and verification process of a customer. Internal controls are applied by obliged entities to some extent (e.g. risk management, record keeping, training). Obliged entities are reporting few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a partial sharing of information. **=> moderately significant vulnerabilities**
SIGNIFICANT (value: 3)	[Within the sector/area considered, deterrence measures and controls have limited effects in deterring criminal/terrorist abuse of the service. The sector shows an organisational framework presenting very significant weaknesses and/or a significant exposure to the risk of ML/TF.]. **Illustrative assessment criteria:** **<u>RISK EXPOSURE</u>** - Significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; few secured and/or monitored delivery channels; significant level of financial transactions; significant cash based transactions; low management of new technologies and/or

	new payment methods - Significant volumes of higher risk customers; low ability to manage corporate entities or trusts in customer relationships - Major part of business and customer is based in areas identified as high risk; significant level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows limited awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, and training, allocated resources). The sector benefits from a limited organisational framework. - Competent authorities provide for a limited ML/TF risk assessment to the sector and LEAs have low capacity to counter ML/TF risks (only some ML/TF cases are visible and unlikely to be detected, leading to few investigations, prosecutions and convictions) - The FIU can detect and analyse the risks only in limited circumstances which allows only a limited functioning of gathering information through STR. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework does not cover the most substantial parts of the risks inherent to this sector. - Controls applied by the sector present significant weaknesses. Few reliable CDD/identification mechanisms are in place and does not allow an effective identification and verification process of a customer. Internal controls are applied by obliged entities with very significant weaknesses (e.g. risk management, record keeping, training). Obliged entities are reporting very few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows on few possibilities of sharing of information => **Significant vulnerabilities**
VERY SIGNIFICANT (value: 4)	[Within the sector/area considered, there are extremely limited or no measures and controls in place, or they are not working as intended. The sector shows an organisational framework presenting highly significant weakness and/or a high exposure to the risk of ML/TF]. **Illustrative assessment criteria:** **RISK EXPOSURE** - Very significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; no secured and/or monitored delivery channels; very significant level of financial transactions; very

	significant cash based transactions; no management of new technologies and/or new payment methods - Very significant volumes of higher risk customers[14]; no ability to manage corporate entities or trusts in customer relationships - Business and customer are based in areas identified as high risk[15]; very significant level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows no awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector has no adequate organisational framework to address the ML/TF risks. - Competent authorities don't provide for any ML/TF risks assessment to the sector and LEAs have no ability to counter ML/TF risks (detection is very difficult and there are very few/no financial or other indicators of suspicious activity. The level of investigations, prosecutions and confiscations is extremely low) - The FIU can detect the risks in very limited circumstances or in no circumstances. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework does not cover the risks inherent to this sector - Controls applied by the sector present very significant weaknesses. No reliable CDD/identification mechanisms are in place and the basic identification and verification requirement process of a customer is not fulfilled. Internal controls are not properly applied by obliged entities (e.g. risk management, record keeping, training). Obliged entities are not reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, does not exist or does not allow sharing of information **=> very significant vulnerabilities**

[14] A non-exhaustive list of factors and type of evidence of potentially higher risk customer is included in Annex 3 of Directive (EU) 2015/849

[15] A non-exhaustive list of factors and type of evidence of potentially higher risk countries is included in Annex 3 of Directive (EU) 2015/849. In the same text, Article 9 tasks the Commission to identify high-risk third countries

WORKING ARRANGEMENTS

It is suggested the strategic level of vulnerability for each TF risk will be assessed according to the vulnerability assessment clearing house reconciliation method.

Experts will propose an estimated level of vulnerability for each TF risk identified in step 1/A. Discrepancies in vulnerability estimates will then be discussed multilateral (or bilaterally if needed), until the Commission considers that a common position, deemed as common to the EU as a whole, is agreed. Should a difference of estimates remain these experts will attempt to determine whether the higher vulnerability estimate is primarily due to an estimated higher vulnerability in a specific field or Member State rather than all EU Member States equally. If so, the level of vulnerability which will be retained by the Commission for the purpose of the current methodology will be that which it considers as common to the EU as a whole.

The Commission will have a decisional power to validate the outcomes of the vulnerability **assessment reconciliation method**

STEP 3/B: May-July 2016 – dedicated meeting: assessing the level of vulnerability for each ML risk identified in step 1/B

Location: standard meeting room

COMPOSITION: Member States experts (to be appointed by MS authorities)[16], COM (DG JUST, DG HOME), Europol, ESAs.

OBJECTIVE: based on the outcomes of step 1/B, the meeting should led, for each identified ML risk, to assess its vulnerability level according to a four scale vulnerability level:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

[16] See footnote 3

3) Significant (value: 3)

4) Very significant (value: 4)

SOURCES (non-exhaustive)**:** open sources, inputs from national risk assessment, inputs from Commission services, inputs from Europol, available intelligence from Member States / FIU, inputs from financial sectors supervisors, non-financial sectors supervisors, private sectors, and available statistics from judicial records.

METHODOLOGY: the assessment of the vulnerability level for each identified ML risk as resulting from step 1/B, should led to a vulnerability assessment level common to the EU as a whole as result, among others, of differences between the regulatory frameworks of Member States which might induce vulnerabilities at a supra national level.

The vulnerability assessment will be performed for the areas/sectors, related to the modus operandi identified in step 1B, required to implement the ML legislation. Consideration will be also given to threats which cannot be linked to a sector.

For the specific purpose and scope of the SNRA the vulnerability assessment will consider primarily the existence of national, EU and international legislation and their effective implementation at national level. By taking into account the EU wide nature of the risks to be considered in the SNRA, particular attention should also be paid to other criteria such as the effectiveness of information sharing among FIU, coordination with other AML authorities and international cooperation, including between AML supervisors.

One of the main components of the vulnerability assessment will consider, for each category of sectors, the specific risk and effectiveness of AML safeguards in place.

Table 4: **The vulnerability component will be assessed according to a four scale vulnerability level:**

LOWLY SIGNIFICANT (value: 1)	[Within the sector/area considered, deterrence measures and controls exist and are effective at deterring money laundering and financing terrorism. The sector shows a positive organisational framework and a negligible exposure to the risk of ML/TF]. **Illustrative assessment criteria:** **RISK EXPOSURE** - No or very limited products, services or transactions that facilitate speedy or anonymous transactions; secured and/or monitored delivery channels; low level of financial transactions; low level of cash based transactions; high quality management of new technologies and/or new payment methods - Very limited volume of higher risk customers; high ability to manage corporate entities or trusts in customer relationships - No or very limited business and customer based in areas identified as high risk; low level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows a satisfactory level of awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from a positive organisational framework. - Competent authorities provide a comprehensive ML/TF risk assessment related to the sector and LEAs have a high ability to counter ML/TF risks (a range of ML/TF cases is visible and highly likely to be detected, leading to investigation, prosecution and convictions) - Good ability of the FIU to detect and analyse the risks, to ensure a good functioning of gathering information through STR, in particular through the use of tailor-made indicators and a sufficient amount of resources to actually perform the risk-analysis. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework is commensurate to the risks inherent to this sector. - Controls [defined by the legislation] are effectively applied by the sector. Reliable CDD/identification mechanisms are in place to ensure adequate identification and verification process of a customer. Internal controls are applied by obliged entities in a robust manner (e.g. risk

	management, record keeping, training). Obliged entities are effectively reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a good level of sharing of information **=> Lowly-significant vulnerabilities.**
MODERATELY SIGNIFICANT (value: 2)	[Within the sector/area considered, deterrence measures and controls exist and are reasonably effective at deterring money laundering and financing terrorism. The sector shows an organisational framework presenting some weaknesses and/or an exposure to the risk of ML/TF.]. **Illustrative assessment criteria**: **RISK EXPOSURE** - Limited products, services and transactions that facilitate speedy or anonymous transactions; mostly secured and/or monitored delivery channels; rather significant level of financial transactions; rather significant cash based transactions; good management of new technologies and/or new payment methods - Few higher risk customers; good ability to manage corporate entities or trusts in customer relationships - Some business and customer are based in areas identified as high risk; rather significant level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows some awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from an organisational framework which shows some weaknesses. - Competent authorities provide a reasonable ML/TF risk assessment related to the sector and LEAs have a good ability to counter ML/TF risks (a range of ML/TF cases is visible and likely to be detected, leading to some investigations, prosecutions and convictions - FIU can detect and analyse the risks in certain circumstances, to ensure a good functioning of gathering information through STR, in particular through the use of tailor-made indicators **LEGAL FRAMEWORK AND CONTROLS**

	- The existing legal framework covers in major parts the risks inherent to this sector - Controls [defined by the legislation] are applied by the sector but presenting some weaknesses. Reliable CDD/identification mechanisms are in place but do not ensure systematically an adequate identification and verification process of a customer. Internal controls are applied by obliged entities to some extent (e.g. risk management, record keeping, training). Obliged entities are reporting few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a partial sharing of information. **=> moderately significant vulnerabilities**
SIGNIFICANT (value: 3)	[Within the sector/area considered, deterrence measures and controls have limited effects in deterring criminal/terrorist abuse of the service. The sector shows an organisational framework presenting very significant weaknesses and/or a significant exposure to the risk of ML/TF.]. **Illustrative assessment criteria:** **<u>RISK EXPOSURE</u>** - Significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; few secured and/or monitored delivery channels; significant level of financial transactions; significant cash based transactions; low management of new technologies and/or new payment methods - Significant volumes of higher risk customers; low ability to manage corporate entities or trusts in customer relationships - Major part of business and customer is based in areas identified as high risk; significant level of cross-border movements of funds; **<u>AWARNESS OF THE RISK VULNERABILITY</u>** - Sector concerned shows limited awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, and training, allocated resources). The sector benefits from a limited organisational framework. - Competent authorities provide for a limited ML/TF risk assessment to the sector and LEAs have low capacity to counter ML/TF risks (only some ML/TF cases are visible and unlikely to be detected, leading to few investigations, prosecutions and convictions)

	- The FIU can detect and analyse the risks only in limited circumstances which allows only a limited functioning of gathering information through STR. **<u>LEGAL FRAMEWORK AND CONTROLS</u>** - The existing legal framework does not cover the most substantial parts of the risks inherent to this sector. - Controls applied by the sector present significant weaknesses. Few reliable CDD/identification mechanisms are in place and does not allow an effective identification and verification process of a customer. Internal controls are applied by obliged entities with very significant weaknesses (e.g. risk management, record keeping, training). Obliged entities are reporting very few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows on few possibilities of sharing of information => **Significant vulnerabilities**
VERY SIGNIFICANT (value: 4)	[Within the sector/area considered, there are extremely limited or no measures and controls in place, or they are not working as intended. The sector shows an organisational framework presenting highly significant weakness and/or a high exposure to the risk of ML/TF]. **Illustrative assessment criteria:** **<u>RISK EXPOSURE</u>** - Very significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; no secured and/or monitored delivery channels; very significant level of financial transactions; very significant cash based transactions; no management of new technologies and/or new payment methods - Very significant volumes of higher risk customers; no ability to manage corporate entities or trusts in customer relationships - Business and customer are based in areas identified as high risk; very significant level of cross-border movements of funds; **<u>AWARNESS OF THE RISK VULNERABILITY</u>** - Sector concerned shows no awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector has no adequate organisational framework to address the

	ML/TF risks. - Competent authorities don't provide for any ML/TF risks assessment to the sector and LEAs have no ability to counter ML/TF risks (detection is very difficult and there are very few/no financial or other indicators of suspicious activity. The level of investigations, prosecutions and confiscations is extremely low) - The FIU can detect the risks in very limited circumstances or in no circumstances. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework does not cover the risks inherent to this sector - Controls applied by the sector present very significant weaknesses. No reliable CDD/identification mechanisms are in place and the basic identification and verification requirement process of a customer is not fulfilled. Internal controls are not properly applied by obliged entities (e.g. risk management, record keeping, training). Obliged entities are not reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, does not exist or does not allow sharing of information **=> very significant vulnerabilities**

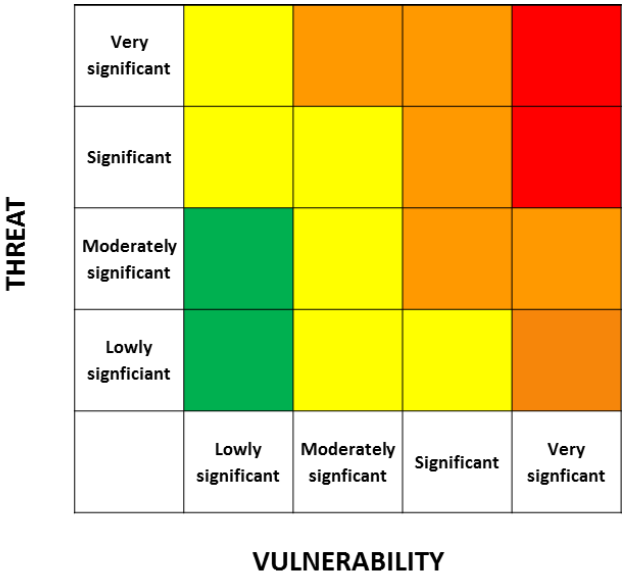
WORKING ARRANGEMENTS

It is suggested the strategic level of vulnerability for each ML risk will be assessed according to the vulnerability assessment clearing house reconciliation method.

Experts will propose an estimated level of vulnerability for each ML risk identified in step 1/B. Discrepancies in vulnerability estimates will then be discussed multilateral (or bilaterally if needed), until the Commission considers that a common position, deemed as common to the EU as a whole, is agreed. Should a difference of estimates remain these experts will attempt to determine whether the higher vulnerability estimate is primarily due to an estimated higher vulnerability in a specific field or Member State rather than all EU Member States equally. If so, the level of vulnerability which will be retained by the Commission for the purpose of the current methodology will be that which it considers as common to the EU as a whole.

The Commission will have a decisional power to validate the outcomes of the vulnerability **assessment reconciliation method.**

STEP 4 (October 2016): Residual risk



The outcomes of steps 2A/B (threat assessment) and 3A/B (vulnerability assessment) will determine the risk level for each identified risk (steps 1A/B), as combination (matrix approach) of the assessed threat and vulnerability level.

The risk level is ultimately determined by combination between the threat *versus* vulnerability. The risk matrix determining this risk level is based on a weighting of 40 % (threat)/ 60 % (vulnerability) - assuming that the vulnerability component has more capacity in determining the risk level. It is assumed that the level of vulnerability is likely to increase the attractiveness and hence the intent of criminals/terrorists to use a given modus operandi – thus impacting ultimately the level of threat.

THREAT

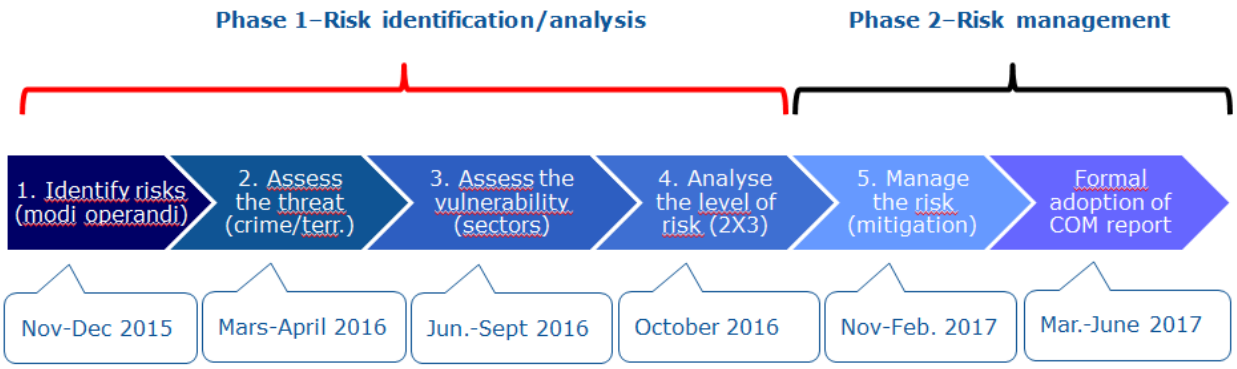
Very significant	2,2	2,8	3,4	4
Significant	1,8	2,4	3	3,6
Moderately significant	1,4	2	2,6	3,2
Lowly signficiant	1	1,6	2,2	2,8
	Lowly significant	Moderately signficant	Significant	Very signficant

VULNERABILITY

RISK

1-1,5	Lowly signficant LOW
1,6-2,5	Moderately signifcant MEDIUM
2,6-3,5	Significant HIGH
3,5-4	Very significant VERY HIGH

SUGGESTED ROAD MAP (summary)



- **November -December 2015:** risks' identification (financing terrorism)
- **November -December 2015:** risks' identification (money laundering)
- **January-February 2016: Private sector/civil society consultation No 1**
- **March-April 2016:** threat assessment (financing terrorism)
- **March-April 2016:** threat assessment (money laundering)
- **May-September 2016:** vulnerability assessment (financing terrorism)
- **May-September 2016:** vulnerability assessment (money laundering)
- **October 2016: consolidated overview of risks**
- **November 2016: Private sector/civil society consultation No 2**
- The road map should also take into account the joint opinion provided by the European Supervisory Authorities on the financial sector to be issued by 26 December 2016

Annex 2

Risk evaluation process

ANNEX 2: Risk evaluation process

The "evaluation" of the identified and assessed risks (outcomes of the risk assessment) is out of the scope of these methodological guidelines. It shall be considered within the framework of the overall risk management process leading to the identification of mitigation measures to fill the identified residual risks. This annex is provided for information purposes only in order to present the output and the procedural steps of the risk evaluation phase.

1. Deliverables

Based on the risk analysis, the Commission will issue a risk assessment report which will consist of:

- A Commission communication including the mitigating measures (max 15 pages).

- A staff working document would complete the "political" input for a more comprehensive presentation of the risk analysis.

- If need be, a classified technical annex may be prepared to protect sensitive information (EU RESTRICTED)

2. Procedural steps

Following the delivery of the risk analysis, the Commission will carry out the following procedural steps (tentative timing only):

- Analyse the results and identify mitigating actions (by end of November 2016)

- Draft the SNRA report (by January 2017)

- Consult EGMLTF and FIU platform about the draft report (by March 2017)

- Formally adopt the SNRA report (by end of June 2017).

Annex 3

Relevant provisions of Directive 2015/849

ANNEX 3: Relevant provisions of Directive 2015/849

Article 2

(…)

2. With the exception of casinos, and following an appropriate risk assessment, Member States may decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing this Directive on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.

Among the factors considered in their risk assessments, Member States shall assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used.

In their risk assessments, Member States shall indicate how they have taken into account any relevant findings in the reports issued by the Commission pursuant to Article 6. (…)

Article 6

1. The Commission shall conduct an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.

To that end, the Commission shall, by 26 June 2017, draw up a report identifying, analysing and evaluating those risks at Union level. Thereafter, the Commission shall update its report every two years, or more frequently if appropriate.

2. The report referred to in paragraph 1 shall cover at least the following:

(a) the areas of the internal market that are at greatest risk;

(b) the risks associated with each relevant sector;

(c) the most widespread means used by criminals by which to launder illicit proceeds.

3. The Commission shall make the report referred to in paragraph 1 available to the Member States and obliged entities in order to assist them to identify, understand, manage and mitigate

the risk of money laundering and terrorist financing, and to allow other stakeholders, including national legislators, the European Parliament, the ESAs, and representatives from FIUs to better understand the risks.

4. The Commission shall make recommendations to Member States on the measures suitable for addressing the identified risks. In the event that Member States decide not to apply any of the recommendations in their national AML/CFT regimes, they shall notify the Commission thereof and provide a justification for such a decision.

5. By 26 December 2016, the ESAs, through the Joint Committee, shall issue an opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector (the 'joint opinion'). Thereafter, the ESAs, through the Joint Committee, shall issue an opinion every two years.

6. In conducting the assessment referred to in paragraph 1, the Commission shall organise the work at Union level, shall take into account the joint opinions referred to in paragraph 5 and shall involve the Member States' experts in the area of AML/CFT, representatives from FIUs and other Union level bodies where appropriate. The Commission shall make the joint opinions available to the Member States and obliged entities in order to assist them to identify, manage and mitigate the risk of money laundering and terrorist financing.

7. Every two years, or more frequently if appropriate, the Commission shall submit a report to the European Parliament and to the Council on the findings resulting from the regular risk assessments and the action taken based on those findings. (…)

Article 7

1. Each Member State shall take appropriate steps to identify, assess, understand and mitigate the risks of money laundering and terrorist financing affecting it, as well as any data protection concerns in that regard. It shall keep that risk assessment up to date.

2. Each Member State shall designate an authority or establish a mechanism by which to coordinate the national response to the risks referred to in paragraph 1. The identity of that authority or the description of the mechanism shall be notified to the Commission, the ESAs, and other Member States.

3. In carrying out the risk assessments referred to in paragraph 1 of this Article, Member States shall make use of the findings of the report referred to in Article 6(1).

Article 9

Third-country policy

1. Third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union ('high-risk third countries') shall be identified in order to protect the proper functioning of the internal market.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 64 in order to identify high-risk third countries, taking into account strategic deficiencies, in particular in relation to:

(a) the legal and institutional AML/CFT framework of the third country, in particular: (i) criminalisation of money laundering and terrorist financing; (ii) measures relating to customer due diligence; (iii) requirements relating to record-keeping; and (iv) requirements to report suspicious transactions;

(b) the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing;

(c) the effectiveness of the AML/CFT system in addressing money laundering or terrorist financing risks of the third country.

3. The delegated acts referred to in paragraph 2 shall be adopted within one month after the identification of the strategic deficiencies referred to in that paragraph.

4. The Commission shall take into account, as appropriate, when drawing up the delegated acts referred to in paragraph 2, relevant evaluations, assessments or reports drawn up by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing, in relation to the risks posed by individual third countries.

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3):

(1) Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;

(b) customers that are resident in geographical areas of higher risk as set out in point (3);

(c) legal persons or arrangements that are personal asset-holding vehicles;

(d) companies that have nominee shareholders or shares in bearer form;

(e) businesses that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(2) Product, service, transaction or delivery channel risk factors:

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

(d) payment received from unknown or unassociated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(3) Geographical risk factors:

(a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;

(c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;

(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

Annex 4

Terminology

ANNEX 4: terminology

Acceptable risk means the level of risk that is acceptable after mitigating the risk. Considering that it is virtually impossible to reduse AML/CTF risk to zero, some ML/TF risks will always remain.

Capability means the (extent of someone's) power or ability to exploit mechanism/process for ML/TF.

Consequence means the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML or TF may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector. As stated above, ideally a risk assessment involves making judgments about threats, vulnerabilities and consequences. Given the challenges in determining or estimating the consequences of ML and TF it is accepted that incorporating consequence into risk assessments may not involve particularly sophisticated approaches, and that countries may instead opt to focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities. The key is that the risk assessment adopts an approach that attempts to distinguish the extent of different risks to assist with prioritising mitigation efforts.

Evaluation refers to the last stage of risk assessment. It involves taking the results found during the analysis process to determine priorities for addressing the risks, taking into account the purpose established at the beginning of the assessment process. These priorities can contribute to development of a strategy for their mitigation.

Intent means the aim or purpose to exploit a mechanism/process for ML/TF.

Internal market comprises an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured (article 26 TFEU).

Money Laundering means the following conduct, when committed intentionally:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such an activity to evade the legal consequences of that person's action;

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;

(d) participation in, association with, attempts to commit and aiding, abetting, facilitating and counselling any of the activities referred to in points (a), (b) and (c).

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

Money laundering and terrorist financing risk assessment means a product or process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand ML/TF risks and serves as a first step in addressing them. Ideally, a risk assessment, involves making judgments about threats, vulnerabilities and consequences.

Residual risk means the inherent risk minus mitigating controls. The residual risk represents the risk remaining after the consideration of controls in place.

Risk means the ability of a threat to exploit vulnerability

Sector means a group of professions and categories of undertakings (financial or non-financial) that may be misused for the purpose of money laundering and terrorist financing. This definition covers at least the following entities:

(1) credit institutions;

(2) financial institutions;

(3) the following natural or legal persons acting in the exercise of their professional activities:

(a) auditors, external accountants and tax advisors;

(b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or immovable property transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:

(i) buying and selling of immovable property or business entities;

(ii) managing of client money, securities or other assets;

(iii) opening or management of bank, savings or securities accounts;

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies, foundations, or similar legal arrangements;

(c) trust or company service providers other than those referred to in points (a) or (b);

(d) estate agents;

(e) other natural or legal persons trading in goods, to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(f) providers of gambling services.

Other professions and categories of undertakings which are covered at national level or which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes may also be covered by this definition.

Supranational risk means a risk of ML and TF affecting the *internal market* which presents common characteristics that could arise in several or in one Member State only and/or that could also have external causes.

Terrorist Financing means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA.

Threat means a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities. *Threat* is described above as one of the factors related to risk, and typically it serves as an essential starting point in developing an understanding of ML/TF risk. For this reason, having an understanding of the environment in which predicate offences are committed and the proceeds of crime are generated to identify their nature (and if possible the size or volume) is important in order to carry out an ML/TF risk assessment. In some instances, certain types of threat assessments might serve as a precursor for a ML/TF risk assessment.

Vulnerabilities means those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at *vulnerabilities* as distinct from *threat* means focussing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes.

Annex 5

Tables of acronymes

ANNEX 5: Table of Acronymes

ML	Money laundering
TF	Terrorist financing
AML/CFT	Anti-money laundering and countering terrorist financing
SNRA	Supranational risk assessment
ESAs	European supervisory authorities
ADHWG	Ad Hoc Working Group
LEA	Law Enforcement Authorities
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit