FATF

FATF GUIDANCE

National Money Laundering and Terrorist Financing Risk Assessment

February 2013

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

Table of Contents

ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIU	Financial Intelligence Units
INR. X	Interpretive Note to Recommendation X
ML	Money Laundering
NPO	Non-Profit Organisation
RBA	Risk-Based Approach
SRB	Self-Regulating Body
STR	Suspicious Transaction Report
TF	Terrorist Financing

1. INTRODUCTION & TERMINOLOGY

1.1 Purpose, scope and status of this guidance

1. Identifying, assessing, and understanding ML/TF risks is an essential part of the implementation and development of a national anti-money laundering / countering the financing of terrorism (AML/CFT) regime, which includes laws, regulations, enforcement and other measures to mitigate ML/TF risks. It assists in the prioritisation and efficient allocation of resources by authorities. The results of a national risk assessment, whatever its scope, can also provide useful information to financial institutions and designated non-financial businesses and professions (DNFBPs) to support the conduct of their own risk assessments. Once ML/TF risks are properly understood, country authorities may apply AML/CFT measures in a way that ensures they are commensurate with those risks – *i.e,.* the risk-based approach (RBA) – which is central to the FATF standards as is set out in Recommendation 1, its interpretive note (INR 1), as well as in other Recommendations (*e.g.,* Recommendations 10, 26 and 28).

2. This document is intended to provide guidance on the conduct of risk assessment at the country or national level, and it relates especially to key requirements set out in Recommendation 1 and paragraphs 3-6 of INR 1. In particular, it outlines general principles that may serve as a useful framework in assessing ML/TF risks at the national level. The guidance contained in this document takes into consideration previous FATF work[1], which is still valid reference material. The general principles contained in this paper are also relevant when conducting risk assessments of a more focussed scope, such as in assessments of a particular financial or DNFBP sector (for example, the securities sector) or of thematic issues (for example, the proceeds of corruption related ML). All of these types of assessments (comprehensive, sectoral or thematic) carried out at the national level may also form the basis for determining whether to apply enhanced or specific measures, simplified measures, or exemptions from AML/CFT requirements. Furthermore, while FATF Recommendation 1 does not create specific risk assessment obligations regarding the financing of proliferation of weapons of mass destruction, the general principles laid out in this guidance could also be used in conducting a risk assessment for this area.

3. The guidance in this document is not intended to explain how supervisors should assess risks in the context of risk-based supervision, although risk-based supervision will likely be informed by a national-level risk assessment. Also, this guidance does not provide further explanation of RBA obligations and decisions for financial institutions and DNFBPs. The FATF has issued separate

[1] See bibliography for a list of relevant FATF work, national-level assessments available online and other relevant material. Annex III contains summaries of selected country-level assessment processes.

guidance on implementing the RBA for specific sectors and professions[2], and that material will be reviewed and, as necessary, modified in light of the revised FATF Recommendations.

This guidance document is not a standard and is therefore not intended to designate specific actions necessary to meet obligations under Recommendation 1 and INR 1 or any other Recommendations dealing with the RBA. Criteria for technical compliance and for assessing effectiveness relevant to this and all other FATF Recommendations may be found in the FATF assessment methodology. The practices described in this guidance are intended to serve as examples that may facilitate implementation of these obligations in a manner compatible with the FATF standards.

4. This guidance is structured as follows:

- This section (1) lays out the purpose, scope and status of this guidance, along with an outline of the core FATF obligations relevant to ML/TF risk assessments at any level.
- Section 2 lays out general principles that should be taken into account when conducting ML/TF risk assessments at the country or national level.
- Section 3 discusses how to organise a national-level ML/TF risk assessment, its frequency, and the data and information that could be used while undertaking such an assessment.
- Section 4 presents a high-level view of the three main stages involved in the ML/TF risk assessment process (identification, analysis and evaluation).
- Section 5 considers the outcome and dissemination of the risk assessment product.
- Annexes to this document contain additional information relating to ML/TF risk assessment including summaries of selected national-level assessments.

1.2 Core FATF obligations and decisions regarding ML/TF risk assessments

5. It is important that the users of this guidance have an understanding of the obligations contained in Recommendation 1 and its interpretive note. This section provides a general outline of these obligations. For more details, reference should be made to the texts of Recommendation 1 and its interpretive note, as well as the FATF assessment methodology.[3]

6. **Recommendation 1:** The text of Recommendation 1 lays out a number of basic principles with regard to risk assessment. First, it calls on countries to "identify, assess and understand" the ML/TF risks they face, and states that countries should also designate "an authority or mechanism to co-ordinate actions to assess risks". The goal of the standard is to ensure that countries can

[2] Nine sectoral RBA guidance papers are available from the FATF website: www.fatf-gafi.org/. This guidance will be revised following adoption of the revised FATF Recommendations in February 2012.

[3] See FATF website (www.fatf-gafi.org) for these texts.

mitigate their ML/TF risks effectively, and the risk assessment is clearly intended to serve as the basis for application of the risk-based approach, *i.e.*, "to ensure that measures … are commensurate with the risks identified." The text of the Recommendation adds that the "[risk-based] approach" (and therefore the risk assessment process on which it is based) should also be "an essential foundation" in allocating AML/CFT resources efficiently. Furthermore, the Recommendation indicates that risk assessments carried out by countries should be used for determining higher and lower risks that may then be addressed by applying enhanced measures or allowing simplified measures respectively. The Recommendation concludes by requiring that financial institutions and DNFBPs should also be able to identify, assess and take effective action to mitigate ML/TF risks.

7. **Interpretive Note to Recommendation 1:** INR 1 provides more details on the requirement for countries to assess their ML/TF risks and on the purposes for which such assessments may be used[4]. In particular, it emphasises that the objective of the risk-based approach is to ensure AML/CFT measures are commensurate with the "risks identified", as well as to enable decision making on effective resource allocation. In elaborating on the specific obligations and decisions for countries, INR 1 states that countries should take steps to identify and assess their ML/TF risks on an "ongoing basis." The objectives of the process at the country level are: (1) to provide input for potential improvements to the AML/CFT regime, including through the formulation or calibration of national AML/CFT policies, (2) to help in prioritising and allocating AML/CFT resources by competent authorities, including through feeding into any risk assessments conducted by such competent authorities (*e.g.*, supervisors) and (3) to feed into the AML/CFT risk assessments carried out by financial institutions and DNFBPs. The text of the interpretive note indicates that supervisors, in accordance with Recommendations 26 and 28, should review the risk assessments prepared by financial institutions and DNFBPs and take the result of that review into consideration in their supervision. The text of INR. 1 also adds that country-level risk assessments should be kept up-to-date, and appropriate information should be shared with all relevant competent authorities, self-regulatory bodies, financial institutions and DNFBPs.

8. In the cases of higher and lower risk determination, country-level risk assessments have very specific roles: Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these risks. Where countries identify lower risks they may decide to allow simplified measures to be applied in relation to some of the FATF Recommendations.

1.3 Key concepts and terms relevant to ML/TF risk assessment

9. In discussing ML/TF risk assessment, it is useful to have a common understanding of certain key concepts and terms that will be used in this guidance. Many of these come from the area of *risk management*, a process commonly used in the public as well as the private sectors to help in decision-making. While many risk management concepts are usefully described elsewhere[5], their

[4] Footnote 1 of INR. 1 specifically acknowledges that supra-national risk assessments should be taken into account, where appropriate. It should be noted therefore that the general principles set out in this document that apply to risk assessments carried out by countries at a national level may also be appropriate to risk assessments carried out at a supra-national level. See Section 2 for further discussion of this issue.

[5] See for example (2009a), ISO (2009b) and ISO (2009c) [see bibliography].

use in this guidance has been adapted to the particular case of assessing ML/TF risk at the national level. Broadly speaking, however, risk management involves developing the appropriate measures to mitigate or reduce an assessed level of risk to a lower or acceptable level.

10. For the purposes of assessing ML/TF risk at the national level, this guidance uses the following key concepts:

- ***Risk*** can be seen as a function of three factors: *threat*, *vulnerability* and *consequence*. An ML/TF *risk assessment* is 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, which are discussed below.
- A ***threat*** is 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.[6]
- The concept of ***vulnerabilities*** as used in risk assessment comprises 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.
- ***Consequence*** refers to 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

6 The United Nations Office on Drugs and Crime (UNODC) has published *Guidance on the preparation and use of serious and organised crime threat assessments* ("The SOCTA Handbook"), which provides useful information on the conduct of national threat assessments related to serious and organised crime.

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.

1.4 Users of ML/TF risk assessments

11. The form, scope and nature of ML/TF risk assessments should ultimately meet the needs of its users – whether these are policy makers, supervisors, operational agencies, financial institutions, DNFBPs, etc. The number and diversity of users of an assessment varies according to the purpose for which it is carried out; however, typical users of risk assessments might include:

- Policy makers and other authorities, for example, in order to formulate the national AML/CFT policies, make reasonable decisions on the legal and regulatory framework and the allocation of resources to competent authorities on the basis of FATF Recommendation 2.
- Operational agencies, including law enforcement, other investigative authorities, financial intelligence units (FIUs), relevant border agencies, etc.
- Regulators, supervisors and self-regulatory bodies (SRBs).
- Financial institutions, and designated non-financial businesses and professions (DNFBPs), for which the national-level ML/TF risk assessment is a critical source[7] contributing to their own ML/TF risk assessments and risk-based obligations.
- Non-profit organisations (NPOs).
- AML/CFT assessors and assessment bodies more broadly, along with other international stakeholders.
- The general public, as well as academia, specified individuals, etc.

[7] According to the FATF standard, countries are expected to make appropriate information on the results of their national risk assessment available to financial institutions and DNFBPs for this purpose.

2. GENERAL PRINCIPLES FOR NATIONAL ML/TF RISK ASSESSMENTS

12. The general principles set out below could be considered when a country intends to conduct any kind of ML/TF risk assessment. These include considerations on the purpose and scope of the assessment as well as the process through which an assessment will be conducted; the stages of a risk assessment, the participants, users and other parties involved; the information which may be used, and the final outcome of the assessment process.

13. The nature, methodology, participants, and information required for an assessment depend on the purpose and scope of the assessment. There is no single or universal methodology for conducting an ML/TF risk assessment. Therefore, this guidance does not advocate the use of any particular methodology or process. This guidance is aimed to provide a generic description of the risk assessment process as it might be applied to looking at risk associated with ML/TF and considerations and practical tools for countries to take into account when undertaking their own ML/TF risk assessment.[8]

2.1 Clear agreement on purpose

14. Before starting any kind of ML/TF risk assessment, all parties involved, including those who will conduct the assessment and, as appropriate, the eventual end users should be in agreement on the purpose and scope of the assessment. Expectations should also be set as to how the results relate to the understanding of national-level risks. Generally, a ML/TF risk assessments is intended to help a country to identify, assess and ultimately understand the ML/TF risks it faces. A country may set out more concrete goals for a particular risk assessment however, such as informing the development of policy or the deployment of resources by supervisors, law enforcement and other competent authorities. Understanding the scale and impact of identified risks can also assist in determining the appropriate level and nature of AML/CFT controls applied to a particular product or sector. Given the diversity of potential users and possible diverging expectations, it is essential at the outset that there be clarity about why an assessment is to be conducted, the questions it should answer, the criteria that will be used to answer those questions and the possible decisions that the assessment will feed into.

15. ML/TF risk assessments may be tied to strategic planning and linked to specific actions or decisions. For example, a national ML/TF risk assessment serves as input to a national AML/CFT strategy or policy as part of the country's domestic AML/CFT co-ordination process. The purposes of the assessment will also vary according to the needs of the users. The purpose and scope of the assessment may also determine the methodology that is to be used.

[8] Nonetheless, those involved carrying out a national ML/TF risk assessment may gain further insight into risk concepts, methodologies, processes, and tools from consulting any requirements of their own government relating to risk assessment or other material on risk management standards and associated publications (see the bibliography at the end of this document for a list of some of these sources).

2.2 Determining scope

Money laundering and terrorist financing

16. A key consideration when deciding on the scope of an ML/TF risk assessment is to determine whether ML and TF risks should be assessed separately or together. Factors associated with TF that might need to be considered may be very different from those associated with ML. For example, funds used for financing of terrorist activities may be derived from criminal activity or legal sources. In addition, a key focus in combating TF is on preventing future terrorist acts from occurring whereas with combating ML, the criminal activity (the predicate offence) has already taken place. Another difference is that, transactions associated with TF may be conducted in very small amounts, which when not viewed in the TF context could be the very transactions that are frequently considered to involve minimal ML risk. Countries may therefore choose to assess their ML and TF risks separately.[9]

National, supranational and sub-national risk assessments

17. As stated throughout this guidance, ML/TF risk assessments may be undertaken at different levels and with differing purposes and scope, including supranational assessments (of a group of countries), national (or country level) assessments and sub-national assessments (of a particular sector, region, or operational function within a country) even though the basic obligation of assessing and understanding ML/TF risk rests on the country itself. In order to be of use in assessing and understanding national-level risks, it is helpful that assessments carried out at other levels relate to each other in a consistent way, although it is recognised that this may not be possible in all instances due to specific risks and the specific assessment approach undertaken. For example, the interplay between a national ML/TF assessment and specific sectoral ML/TF risk assessments could be considered as follows:

- High or low risk situations identified by the competent authorities through national ML/TF assessment should logically influence and/or confirm choices of higher, lower, or low risk situations relevant to the risk-based approach as implemented by financial institutions and DNFBPs, and overseen by supervisors or SRBs.
- Continuing examination by financial institutions and DNFBPs of their risks (regarding types of customers, products, etc.) as monitored by supervisory agencies would potentially contribute to and/or confirm identification of risk levels in the context of national ML/TF assessments.

18. In principle, a national ML/TF risk assessment can be composed of different types of assessments, and the different levels could be combined together to form a national-level understanding of the risk with each limited-scope assessment contributing to the overall picture. It may, for example, be possible for those conducting the ML/TF assessment to rely on a variety of assessments (for example, assessments conducted by supervisors and SRBs on the ML/TF risks in

[9] For the purposes of ML/TF risk assessment, this guidance discusses indicators or elements relating to ML and TF in Section 4 under the explanations of identification and analysis. Further relevant lists are provided in Annexes I and II.

financial and DNFBPs sectors, ML/TF risk assessments conducted by the firms operating in the financial and DNFBP sectors, threat assessments conducted by law enforcement agencies and FIUs on ML[10] and TF, assessments of the ML/TF vulnerabilities in the NPO sectors or legal persons and arrangements, and any ML/TF assessments carried out at the state level in a federation) to form a national-level understanding of the ML/TF risk.

19. The approach adopted by each country may also be dependent on the country's framework for co-ordinating and co-operating on AML/CFT matters. For example, in some cases, it might be more appropriate to pull together all or many of the relevant contributors to conduct a single national ML/TF risk assessment. This would also simplify the need to collate and compare different types of assessments and allow for more direct exchange of information between the contributors. In other cases, where the ML/TF risks are diverse and differ between regions, or where the competent authorities have to deal with very specific risks or need to conduct an assessment to justify exemptions on the basis of low ML/TF risks, it may be more appropriate to have targeted, sectoral or thematic risk assessments which the national authorities would then use in developing a national-level understanding of the ML/TF risks.

20. The size and complexity of the country, its ML/TF environment, and the maturity and sophistication of the AML/CFT regime may also influence how a country decides to assess and understand its ML/TF risks. Ideally, a national-level ML/TF assessment should attempt to focus on macro-level risks affecting the AML/CFT regime. For example, it may focus on the potential abuse of sectors rather than of individual institutions, or the adequacy of resources across a linked group of AML/CFT competent authorities rather than individual authorities, and so on. The degree of aggregation or disaggregation of risks to focus on will be country specific.

Comprehensiveness of assessment

21. Regardless of the approach adopted, countries are advised to ensure that their assessment of ML/TF risk is comprehensive enough to provide an overall picture of the national ML/TF risks across the AML/CFT regime. Ideally, this picture should include sufficient breadth and depth about potential threats and vulnerabilities and their consequences to address the purpose and scope of the assessment. The range of threats and vulnerabilities relevant for any particular assessment will thus vary according to the scope of the assessment (national, regional, sectoral, etc.); however, the country will need to ensure that all relevant risks are taken into account when the results from different types of assessments are combined to derive national-level ML/TF risks. Where information gaps exist or difficulties in reaching conclusions arise, it is useful if these can be recognised in the risk assessment and then become areas where more work is required in the future. In addition, the uncertainty caused by the lack of information may itself raise the risk profile of the issue under consideration. In seeking to develop a comprehensive picture, those in charge of the ML/TF risk assessment need to identify and acknowledge these limitations as they make a determination of the risks that can be assessed. Future risk assessments may be able to seek new or alternative sources of information that will permit assessment of areas that could not be adequately or fully assessed in an earlier work.

10 Again, UNODC (2010) mentioned above may be relevant in this regard.

2.3 Need for high-level commitment to the ML/TF risk assessment process

22. Before conducting an ML/TF risk assessment, it is essential that there be the political will to carry out this work and ensure that the objectives of the assessment can be achieved. This political will may be demonstrated in a clear commitment from high-level government officials to the ML/TF risk assessment exercise. These officials will need to recognise, understand and acknowledge any ML/TF risks that exist within their country and how these risks may be distinct from larger criminal or terrorism related threats. Situations where government officials (or competent authorities) purposely fail to identify ML/TF risks in their country (or they deliberately determine certain risks as low level) because they believe that acknowledgement of a higher risk level may damage their reputation or may have a negative effect on investment within the country and its financial sector need to be avoided.[11] Appropriate judgment and balance are therefore important in the conduct of the national ML/TF risk assessment process to prevent the process from becoming unduly influenced by or subordinate to a particular policy approach, legislative reform, agency agenda, resource injection, or lobbying by a specific stakeholder.

[11] Examples of situations where ML/TF risks are often not acknowledged include those where a country itself may have little criminal or terrorist activity but its vulnerabilities attract foreign funds for laundering or financing activity or its residents send funds abroad to support foreign terrorists and terrorist groups.

3. ORGANISATION AND INFORMATION

3.1 Planning and organisation of the ML/TF risk assessment

23. In establishing a ML/TF risk assessment process, some countries may choose to establish a more formal inter-agency working group or the like to oversee their risk assessment process. Round-table discussions, working groups of experts and taskforces of relevant agencies and bodies are other examples of how such a process may be organised. It is useful if the process is as inclusive and co-operative as possible. However, ideally there should be a clear determination and designation of the specific agency, organisation or "task force" in charge of leading and co-ordinating the process. See Annex III which contains examples of national-level assessments for specific ways that countries have organised their assessments.

24. As mentioned in the previous section, the purpose and scope of the particular assessment will likely determine the composition of the risk assessment "team". Meetings, interviews, data gathering, and analysis related to national-level ML/TF risks can be a lengthy process, particularly if there is disagreement among competent authorities on the threats and vulnerabilities. A clear project plan describing the process, roles and responsibilities of various partners for identifying, assessing and understanding the country's ML/TF risks may therefore be useful. In addition, an appraisal of likely resource requirements needed to undertake the ML/TF risk assessment may be beneficial.

25. There are a variety of processes through which a country may reach an informed understanding of the risks it faces – in a particular situation or overall. This includes top-down approaches (resulting from a single, co-ordinated framework or system) and bottom-up (building a national assessment from a patchwork of assessments with a smaller scope). It also includes organic processes which may develop an understanding of risk incrementally, for example by starting with a limited or specific focus assessment and gradually expanding it whilst learning from the experience of the preceding work.

3.2 Sources of information

Contributors to the risk assessments

26. While some aspects of the ML/TF risk assessment may be conducted through a single agency process, in most cases, it is unlikely that one organisation by itself possesses all necessary information and data to adequately perform such a task at the national-level. It is therefore advisable that a national-level ML/TF assessment exercise involve a broad range of relevant departments, agencies and other organisations within the government (federal and other levels as applicable) that have AML/CFT responsibilities, expertise or both. This includes those with knowledge of the types and scope of proceeds-generating offences, those that can identify AML/CFT regime vulnerabilities and those with other critical related information. Contributors that may provide essential input to the national-level ML/TF risk assessment process include the following (see also Figure 1):

- *Policy-making bodies*: Policy making bodies should, where relevant, be included in the conduct of a risk assessment – not necessarily as providers of information, but as the principal users of risk assessments – in order to ensure that risk assessments adequately address high-level questions and that any implications of the risk assessment for the revision of national AML/CFT policies are identified. They have a particular role to play in helping frame the scope of the risk assessment exercise.
- *Law enforcement and prosecutorial authorities* (including police, customs/border control, and criminal intelligence agencies where appropriate): These operational authorities may be able to provide information on specific cases involving the particular area under assessment and may also assist, where possible, in estimating amounts of proceeds of crime based on information on predicate offence. They thus are likely to play a central role as a source of information for the process. They may also have relevant statistics on ML/TF investigations, prosecutions and convictions, assets seized / confiscated / repatriated / shared and other (international) co-operation requests or hold information about criminals' *modus operandi* obtained during the course of an investigation. They may also be able to provide information on new trends and risks detected through their investigations as well as assist in identifying vulnerabilities.[12]
- *Intelligence and/or security services*: These agencies may be particularly relevant to assessments of terrorism and terrorist financing, where much of the available information on threats may come from intelligence sources[13]. Such agencies may also function as centres of expertise on intelligence analysis, and can provide external review or validation of risk or threat assessments using intelligence analysis and assessment methodologies, where these are available. They may also be able to assist in identifying vulnerabilities.
- *Financial intelligence units*: On the basis of the suspicious transaction reports (STRs) and other information it receives and the strategic analysis it conducts, the FIU is ideally placed to identify threats, vulnerabilities, ML/TF techniques, methods and trends, including new patterns[14]. FIUs may be able to extract from their databases information on specific products or transaction types that can be either converted into sanitised cases and/or

12 Some of this information may be available from other authorities such as Justice Ministries and other agencies.

13 However, this may involve information of a sensitive nature which could limit the exchange by intelligence or security services.

14 See INR 29 which describes the role of the FIU in conducting strategic analysis and its role in helping establish policies and goals for other agencies within the AML/CFT regime. At the same time, it may be advisable not to rely too heavily or solely on FIU statistics as these often derive from suspicion about potential ML or TF activity rather than actual cases.

aggregated to reveal a trend. This information can be supplemented by statistics on the reporting of transactions by the reporting entities.

- *Regulatory and supervisory authorities* (including, for example, self-regulatory bodies and any FIUs with such responsibilities) often have the benefit of having a good picture of the institutions regulated for AML/CFT within their countries. Through their AML/CFT inspection and monitoring, either on-site or off-site, they gain a unique knowledge of specific vulnerabilities associated with types of institutions, products, transactions (including those of a cross-border nature) and customers that can be associated with ML/TF and are able to assess a sector's policies, procedures and controls. They are therefore in a position to provide views on whether a particular risk is being adequately identified and managed.
- *Other authorities* such as Foreign Ministries (for example, threats identified by the UN) or statistics agencies may also hold information that can inform the risk assessment exercise and could participate directly or indirectly. Likewise, agencies that may have information about particular criminal activities or predicate crime may also be able to contribute (for example, welfare ministries in relation to welfare fraud, tax authorities in relation to tax crimes, anti-corruption agencies in relation to corruption etc.).
- *International and foreign partners*: FATF-style regional bodies (FSRBs) of which a country is a member may also be a useful source of information on risk, in particular regarding work carried out elsewhere in the region to identify and understand risk. Similarly, foreign partners, such as authorities from other countries, may also be a potential source of information.

Involvement of the private sector and other actors

27. Private sector involvement may also be valuable in building a complete picture of national ML/TF risks and may benefit the assessment process in a number of ways – as either as a source of information or by having representatives participating directly in some aspects of the process if the country considers that appropriate. It is also important to consider that sometimes the private sector may have commercial interests that might preclude a completely impartial view of ML/TF risk. Therefore, while the private sector may not in all countries be an active participant in the national ML/TF assessment, it may be the best source of information in many areas. Contributors from the private sector that may provide essential input to the national-level ML/TF risk assessment process include the following:

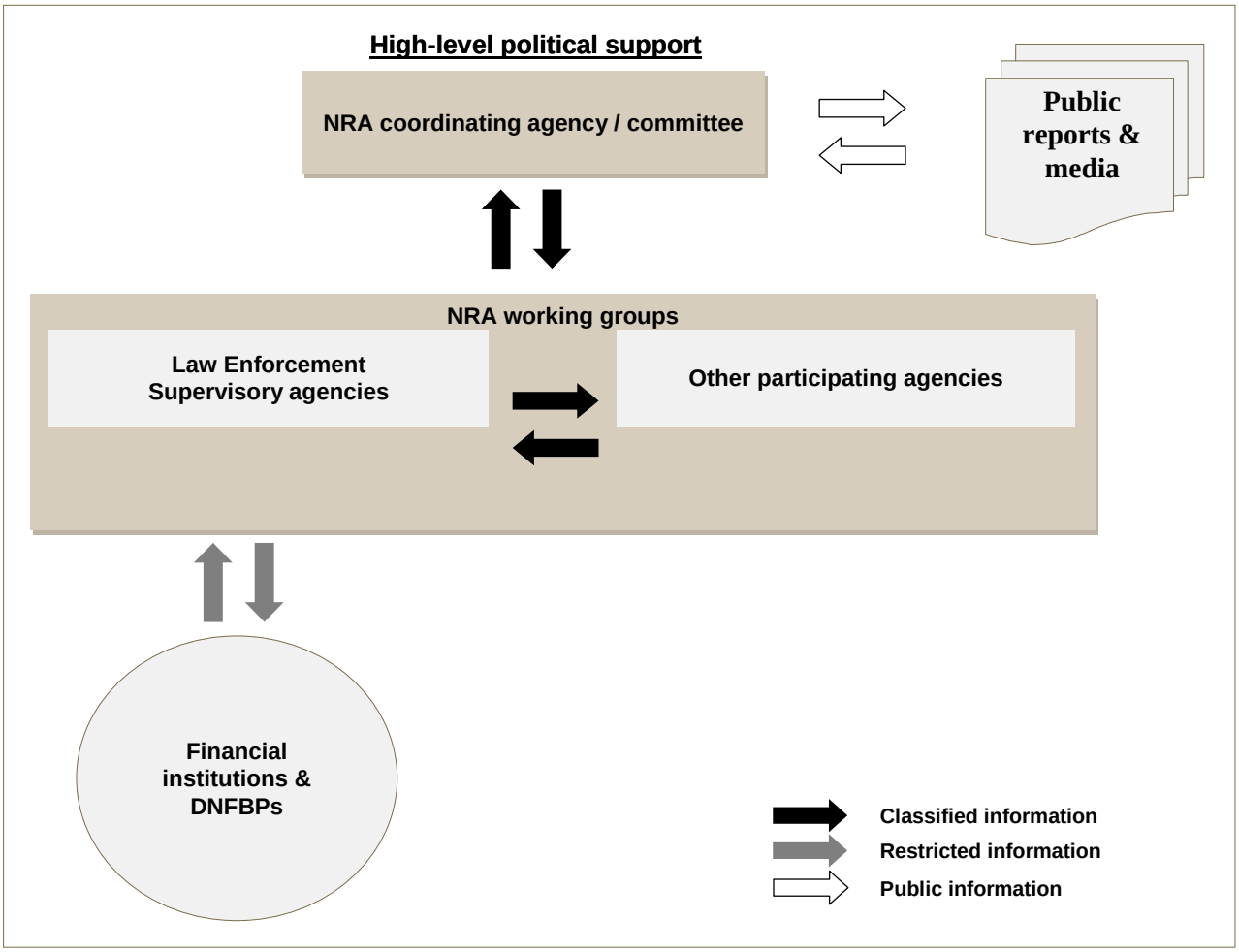
- *Financial institutions and DNFBPs:* When applying the risk based approach to implementing AML/CFT preventive measures, financial institutions and DNFBPs may have already conducted ML/TF risk assessments of their own, and such assessments could also be an important contribution to national-level assessments. More generally, financial institutions and DNFBPs and their staff or representatives may have valuable information on the structure, organisation and size of sectors, their customers as well as the

features and characteristics of particular financial products to help with determining the level of risk presented and to assist in identifying vulnerabilities. As stated in the introduction, the private sector is also a potential key user of any ML/TF risk assessments conducted at national level. It should be noted as well that Recommendation 1 now requires countries to have mechanisms to provide appropriate information on the results of national ML/TF risk assessments to financial institutions and DNFBPs.

- *Industry associations and self-regulatory bodies (SRBs)* with a broad and representative membership in the area of the assessment may provide essential aggregated statistics, such as particular types of transaction volumes and industry-wide information.
- *Other actors*: researchers, criminologists, industry associations, private sector experts (for example, practitioners or others with in-depth knowledge of specialised financial activities), risk management experts, non-government organisations and civil society, academics and other international experts/specialists can provide their perspectives, for example, on what constitutes a "cash intensive" business or economy, produce reports and provide analysis related to ML/TF and predicate crimes. It may be very useful to develop risk assessment methods and the monitoring of the risk assessments by actors with expertise in scientific research.
- *Criminals* could also be a valuable source of information, particularly in jurisdictions where they are given the incentive to "repent" or share information in return for favourable treatment in the criminal justice system. They can explain the reasons why one sector or product or transaction or (more broadly) *modus operandi* was chosen rather than another. While it may be difficult to obtain such information from them directly, there may be indirect methods such as obtaining copies of research into their behaviour or working with prison or custodial authorities to obtain valuable information that they may hold. Court reports, sentencing and transcript records can also be a rich source of information on the motives and methods used by money launderers and terrorist financiers.

28. As a targeted ML/TF risk assessment may focus on a specific sector, only a small number of private sector representatives (for example, from an industry association or SRB) might be involved. A comprehensive national risk assessment on the other hand is of a larger scope and could attract more participation from a wider segment of the private sector. Time and resources to co-ordinate input and obtain agreement among participating bodies need to be considered when planning to undertake large-scale ML/TF assessments that involve extensive consultation.

Figure 1. **Interrelationships between various contributors to the risk assessment process**



Information and tools required for ML/TF risk assessments

29. The quality of the risk assessment exercise depends largely on the types and quality of data and information available. While quantitative assessments (*i.e.*, based mostly on statistics) may seem much more reliable and able to be replicated over time, the lack of available quantitative data in the ML/TF field makes it difficult to rely exclusively on such information. Moreover, information on all relevant factors may not be expressed or explained in numerical or quantitative form, and there is a danger that risk assessments relying heavily on available quantitative information may be biased towards risks that are easier to measure and discount those for which quantitative information is not readily available.

30. For these reasons, it is advisable to complement an ML/TF risk assessment with relevant qualitative information such as, as appropriate, intelligence information, expert judgments, private sector input, case studies, thematic assessments, typologies studies and other (regional or supranational) risk assessments in addition to any available quantitative data. Similarly, objective data can be complemented by surveys or information of subjective nature such as perception indexes. Countries may in the long term wish to consider harmonising and further developing their quantitative data collection mechanisms that are used for ML/TF risk assessment in line with the FATF Standards (for example, Recommendation 33) and international best practices. It is essential

that all participating organisations be authorised to share potentially sensitive information. Such information should be received, exchanged and used in accordance with agreed procedures, policies and applicable laws and regulations.

31. Determining the sources of data, type of information, tools, and which analytical techniques will be used is therefore essential in conducting ML/TF risk assessments. In order for a national ML/TF risk assessment to arrive at the most accurate findings, it is advisable that as much analysis and conclusions within the assessment as possible be based on objective information. The information used in a ML/TF risk assessment may be derived from various sources (both qualitative and quantitative). The availability and quality of information will vary considerably by country. Countries, including low capacity countries, with limited data on criminal investigations or financial transactions will still be able to conduct a risk assessment but may need to rely more on expert judgment and international sources of data after they have obtained all available data from national sources. More generally, some officials may find it beneficial to engage independent experts with substantial experience in risk assessment to carry out some aspects of the risk assessment rather than try to carry out the whole process themselves.

32. A national ML/TF risk assessment may conclude that one of the significant vulnerabilities is the presence of information gaps within the AML/CFT regime that need to be closed. Thus, the risk assessment can also reveal the adequacy of the available data and give directions for potential data and information sources, as well as future data collection requirements. A review of the available data and information within a country's AML/CFT regime as an essential component of the ML/TF risk assessment process also helps identify the extent to which any lack of data and information is a systemic vulnerability in the country.

33. Maintaining a consistent approach to the risk assessment process and using the same quantitative and qualitative indicators where possible is important to enable a comparison of findings over time. However, the desire to compare results between one assessment and the other or after periodic updates should not override the need to improve the methodological process or add new data sources as appropriate. Indeed, the experience obtained from conducting an ML/TF risk assessment – when properly documented – may help a country to refine future assessments or adopt an entirely new and more effective approach in subsequent assessments.

34. When looking at money laundering and terrorism financing trends, a country's international financial transactions may also be a key element. Information on cross-border financial flows is a valuable source of data which needs to be considered. In addition, a number of countries have extensive reporting processes on crimes related to money laundering, such as human trafficking or organised crime and some international organisations collate statistics on these and other relevant crimes. These reports can be an important source of information for assessing national ML/TF risks.

3.3 Other planning considerations

Frequency of the risk assessment

35. Recommendation 1 requires that countries assess risks "on an ongoing basis", and that they keep assessments up-to-date. The authority or mechanism designated to assess ML/TF risks in the

country will likely be responsible for ensuring that this obligation is met. Recommendation 1, however, does not specify a particular period of time. Therefore, the frequency with which a risk assessment is updated is determined by the country, based on a number of factors, including how quickly (and how significantly) the risks may change.

36. Following the initial assessment of a specific area, the entire process does not necessarily need to be repeated at pre-specified points in time. However, it is advisable that the authority or mechanism designated to assess ML/TF risks proposes after the first national-level ML/TF risk assessment when the next risk assessment should be carried out, for example, within the next three to five years. It should also be emphasised that carrying out an ML/TF risk assessment should be considered as an evolutionary process. As indicated above, the lessons learned from an initial risk assessment may help to inform subsequent updates or future risk assessments, and this may also be a factor in determining the frequency.

37. Some factors that could also influence the need for updating or conducting a new ML/TF risk assessment process include: when new ML or TF activity causes substantial harms to occur, or new intelligence or typologies become available or where significant changes are made to products and services (including their operating environment). A number of developments (domestically and internationally) may also prompt the need to review a risk assessment:

- Changes in international standards or guidance (for example, FATF recommendations, IOSCO, IAIS, guidance and sound practice papers issued by the Basel Committee on Banking Supervision, UN Conventions, EU legislation).
- Changes in the political, economic or legal framework of a country.
- Developments in other countries' regimes (in particular the country's important trading partners or countries with similar financial sectors or legal systems).
- Issues raised by the private sector (for example, "level-playing field", "countries of concern" not already identified by FATF, new products, services and technologies).
- Open source material or public reports (for example, FATF typology reports) on new ML or TF trends.
- Domestic typologies studies and intelligence received from law enforcement, the FIU and other stakeholders, which may include updates on the vulnerability of a product or service.
- Information about trends in other countries (by means of international conferences, regular information exchanges, etc.).
- The cycle of mutual or self-evaluation may also be an important consideration for countries in deciding when to conduct or update their risk assessment.

Documentation of methodologies and processes used

38. Regardless of the method or process used to conduct the ML/TF risk assessment exercise, it is advisable that the designated authority or mechanism responsible for assessing a country's ML/TF risks record sufficient information about the methodologies and processes to be used. This is to ensure that all parties involved in the process are aware of their obligations and responsibilities and to assist with demonstrating to other stakeholders, including assessors, how the risk assessment was conducted. Such an approach is also appropriate for the purposes of transparency and accountability.

39. While not all the information and analysis of the risk assessment may be shared broadly, it is essential that the designated authority in charge of co-ordinating the process ensure that adequate records of the data, information, analysis and conclusions are kept securely. Such records allow for the preservation of institutional memory and in explaining the rationale for past risk-related policy decisions, permit future updates, and ensure the consistency in future risk assessments endeavours. Countries can use this body of information to inform AML/CFT assessors about the adequacy of their risk assessment process, subject to restrictions on sharing sensitive information.

Supra-national risk assessments

40. Assessments conducted at a supra-national-level may be of value in country-level or national risk assessments. Such assessments may serve as an additional source of information in conducting risk assessments at the country level and could, for example, help in the identification of threats, vulnerabilities and their consequences. They may also provide a benchmark for certain judgments made in subsequent risk assessments at the country level. It is also worth noting that supranational assessments can themselves be informed by the results of country-level risk assessments.

Links with global ML/TF assessment

41. The FATF Global Money Laundering and Terrorist Financing Assessment was adopted by the FATF in June 2010. The Global ML/TF Assessment provides an overview of the ML/TF threats as identified by the FATF (and therefore on a worldwide or "global" level) along with the ultimate harms that they can cause. The aims of the Global ML/TF assessment are to inform governments, the private sector and international policy-makers about ML/TF threats in order to better manage scarce resources and to take more focused actions against ML/TF. The issues identified in the assessment may be useful to governments when conducting national ML/TF assessments. The Global ML/TF Assessment may therefore provide an important part of the context for any assessments undertaken at national level.

42. Only a few countries have previously carried out national risk assessments, but it is envisaged that the production of national-level risk assessments will become a more important contributor to the Global ML/TF Assessment effort. Therefore there is a two-way relationship between this assessment and national ML/TF risk assessments with each benefiting from information contained in respective assessments.

4. STAGES OF ML/TF RISK ASSESSMENT

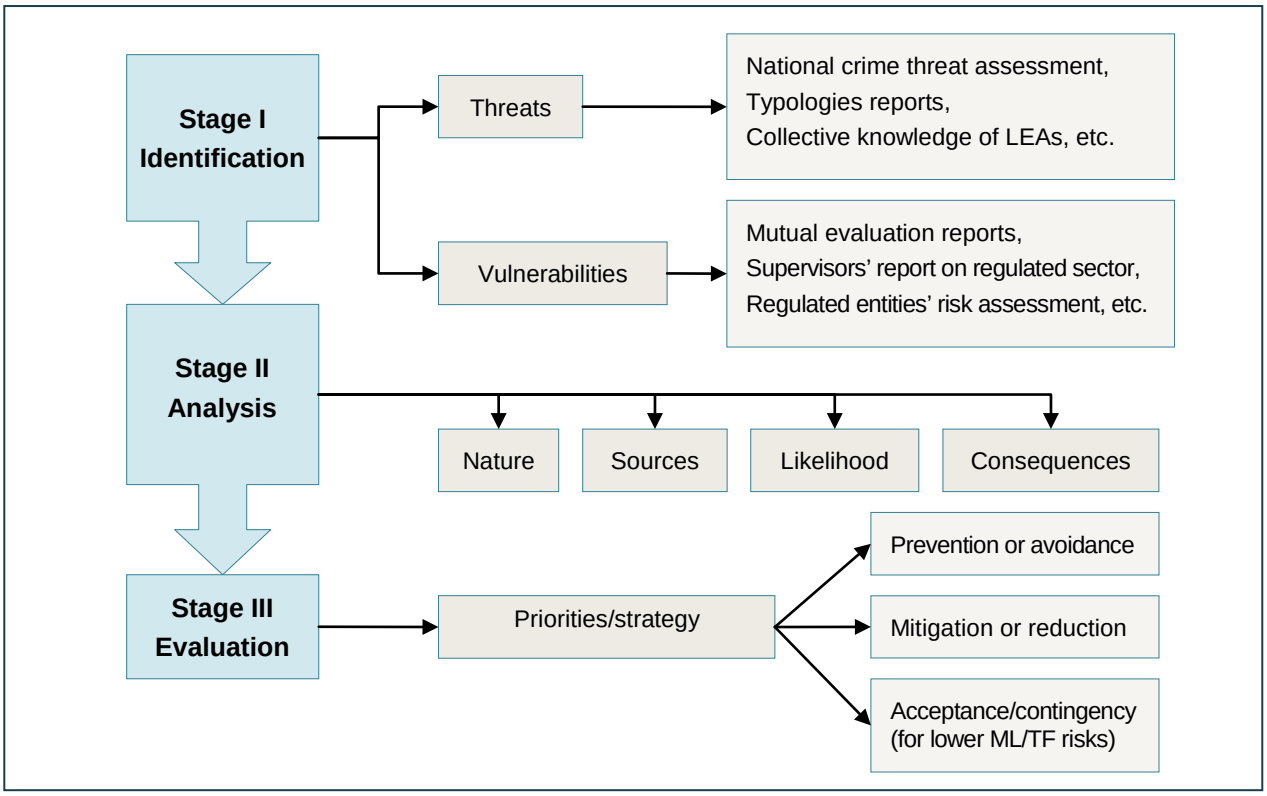
43. The process of risk assessment can be divided into a series of activities or stages: *identification*, *analysis*, and *evaluation*. The three stages are briefly described in this section. For completeness all three stages are described; however, this guidance focuses mainly on the first two. Figure 2 below provides an overview of the ML/TF risk assessment process.

- In general terms, the process of ***identification*** in the context of an ML/TF risk assessment starts by developing an initial list of potential risks or risk factors[15] countries face when combating ML/TF. These will be drawn from known or suspected threats or vulnerabilities. Ideally at this stage, the identification process should attempt to be comprehensive; however, it should also be dynamic in the sense that new or previously undetected risks identified may also be considered at any stage in the process.
- ***Analysis*** lies at the heart of the ML/TF risk assessment process. It involves consideration of the nature, sources, likelihood and consequences of the identified risks or risk factors. Ultimately, the aim of this stage is to gain a holistic understanding of each of the risks – as a combination of threat, vulnerability and consequence in order to work toward assigning some sort of relative value or importance to them[16]. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk and the purpose of the risk assessment, as well as based on the information, data and resources available.
- ***Evaluation*** in the context of the ML/TF risk assessment process involves taking the risks analysed during the previous stage to determine priorities for addressing them, 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.

15 The term *risk factors* is used to refer to specific threats or vulnerabilities that are the causes, sources or drivers of ML or TF risks.

16 As stated in Section 1 under the descriptions of relevant concepts, a risk assessment at the conceptual level involves gaining a comprehensive understanding of all three components of ML/TF risk (threat, vulnerability *and* consequence). The practical challenges in describing ML/TF consequences in a meaningful way may lead countries to focus first and foremost on identifying ML/TF threats and vulnerabilities. The recognition that there are specific consequences of ML/TF threats and vulnerabilities is nevertheless important, as this component, even if understood at a theoretical level may help in assigning a relative value or importance to various ML/TF risks.

Figure 2. **Overview of the ML/TF Risk Assessment Process**



4.1 First stage: identification

44. After establishing the purpose and scope for the risk assessment exercise, a first step is to identify risks to be analysed. Given that ML/TF risks – as stated earlier in this guidance – are a combination of threats, vulnerabilities and consequences, a good foundation for the identification process is to begin by compiling a list of the major known or suspected threats and vulnerabilities that exist based on primary methods and payment mechanisms used, the key sectors which have been exploited, and the primary reasons why those carrying out the ML/TF are not apprehended and deprived of their assets. The identified ML/TF threats or vulnerabilities should of course relate to the purpose and scope of the assessment and this will also influence whether they are more micro or macro in focus.[17]

45. At this initial stage, the list may be broad or specific, be based on actual or known typologies, or drawn from a more generic list of types of cases or schemes or circumstances involved in the ML or TF processes. For ML/TF threats, the development of a list may be facilitated by having access to, for example, national crime threat assessments[18], typologies reports, as well as the collective

17 Decisions will need to be made about the level of aggregation or detail with which the list of threats and vulnerabilities is expressed (along with the risks derived from them), and this will be influenced by the size and complexity of the country. A more focussed ML/TF assessment will typically involve a narrower range risks but it may provide more opportunity for those to be expressed using a higher level of detail than for a national level assessment.

18 Again, the UNODC (2010) mentioned above may be relevant in this regard.

knowledge of law enforcement. Formulating a list of the country's major ML/TF vulnerabilities will typically be informed by the likes of mutual evaluation reports[19] of compliance with the FATF Recommendations[20], reports by supervisors and about vulnerabilities in the regulated sector, risk assessments prepared by regulated entities, and the collective knowledge of the authorities involved in AML/CFT, particularly regarding the existence and effectiveness of any general mitigants or controls that help combat ML/TF (such as limits on cash use in certain transactions) and any weaknesses in how they carry out their responsibilities, including because of a lack of resources. The exercise of establishing this first list of threats and vulnerabilities should consider the full process of ML or TF, including the international/cross-border context. Thus, discussion of ML or TF threats will probably need involvement of appropriate experts who contribute to compiling this initial list of the main or common ML/TF threats and vulnerabilities.

46. ML/TF risks exist when ML/TF threats exploit ML/TF related vulnerabilities. Thus after compiling a list of ML/TF threats and vulnerabilities, the next focus is for those involved in the process to think about how these interact and articulate a list of risks the country faces when combating ML/TF.[21] It should be stressed that something identified on the list at this stage is not automatically classified as having higher (or lower) risk – it has simply been identified as sufficiently relevant to go into mix of risks to be analysed.

47. There are different approaches that may be used at the identification stage. One is based on identifying risk *events*, which involves starting from specific examples of ML or TF events – which may be macro or micro in nature. Under this approach the participants identify the main risk scenarios to analyse. Some examples of specific ML/TF risk events (derived from the threats, vulnerabilities and consequences) identified at this stage might include the following[22]:

- "Organised crime groups place proceeds of crime into the financial system through co-mingling cash with legitimate business takings."
- "Narcotics trafficking groups use cash smuggling to move illegal proceeds over the border."
- "Terrorist group X is known to raise funds via cash donations obtained within the country."
- "Foreign terrorist groups uses domestic NPOs as fronts for terrorist financing activities."

---

19 And detailed assessment reports.

20 Any of these reports may contain outdated information due to the length of time since the last assessment. This material may therefore be supplemented by other material developed through subsequent follow-up or monitoring processes.

21 Some country ML/TF risk assessment processes may wish to move straight to articulating a list of ML/TF risks without identifying threats and vulnerabilities separately

22 See Annex I for a more lists of examples of predicate offences (threats) for money laundering and see Annex II for a list of vulnerability related factors. These may be of assistance in developing lists of threats, vulnerabilities, and consequences during ML/TF risk assessments. It is important to note however that these lists are not exhaustive.

- "Foreign criminal groups launder foreign proceeds of crime in the country by investing in the domestic real estate sector."
- "Criminals and terrorists exploit the lack of information on beneficial ownership and control of companies to obscure or hide links between them and legal persons controlled or owned by them."
- "Terrorists / criminals move funds out of the country via informal money transfer businesses."
- "Financial institutions fail to identify suspicious transactions because of poor monitoring systems."
- "Law enforcement fails to investigate ML due to their focus on predicate crime only."
- "Launderers avoid conviction due to poorly drafted ML laws."
- "Law enforcement are unable to investigate some ML and TF cases due to poor information about beneficial ownership and control of companies used by launderers and financiers."
- "Confiscation of proceeds of crime fails because law enforcement fail to use provisional measures to freeze or seize assets during investigations."

48. Another approach that may be used starts from a macro-level and tends to focus more on circumstances. Under this approach a list of risk factors (relating to threats and vulnerabilities, see Annexes I and II for some examples of risk factors) is identified for analysis. The list can be expanded or narrowed down depending on the scope of the ML/TF assessment.

49. Irrespective of which approach is used for identification, those involved in the process must keep an open mind to ensure that all relevant risks or risk factors are identified so as to avoid inadvertently overlooking key issues that contribute to the country's ML/TF risk. The actual processes used to identify the initial list of risks will vary. Some countries may utilise more formal techniques such as surveys and quasi-statistical analysis of past events or circumstances while others may carry out a brainstorming exercise among appropriate experts to produce a list or perhaps a tree diagram of related events or circumstances. Once an initial list of risks is identified, the assessment process can proceed to the next stage.

4.2 Second stage: analysis

50. *Analysis* lies at the heart of the ML/TF risk assessment process. It is through analysis that the process moves from a mere description of the ML/TF risks facing a country – akin to a situation report – to fuller understanding of the nature, extent and possible impact of those ML/TF risks. As indicated in the introduction, risk can be thought of as a function of *threat*, *vulnerability* and *consequence*. The goal of this step is therefore to analyse the identified risks in order to understand their nature, sources, likelihood and consequences in order to assign some sort of relative value or importance to each of the risks.

51. Ideally, such analysis takes into account the relevant "environmental" factors -- in the broadest sense -- which influence how the risks evolve. These broad "environmental" factors include the general circumstances of the country (for example, relevant political, economic, geographical and social aspects), as well as other structural of specific contextual factors which could influence the way AML/CFT measures are implemented. Determining which environmental factors are relevant to ML and TF (and thus influence the nature, sources, likelihood and consequences of the identified risks) can be assisted by thinking of them in terms of the political, economic, social, technological, environmental and legislative factors that may enable or facilitate the particular risk. In practical terms, many of these factors will have already been identified as among some of the vulnerabilities facing the country (See Annex II).

52. In practice, not all broad environmental factors will be applicable to every ML/TF risk assessment. Indeed, the individual factors will vary from country to country and may evolve over time. It is important to ensure that factors looked at are indeed relevant, and it may therefore be necessary to use some of the methods (surveys, brainstorming) mentioned above to agree on which factors to consider in a particular ML/TF assessment process. In addition, it may become apparent in thinking about some of these factors that certain ML/TF risks might not have been identified at the first stage. As stated previously, the process – even at the analysis stage – should be flexible enough to make adjustments to modify (add to, delete or combine) the risks identified in stage one of the process.

53. Having considered the influence of the broad environmental factors on each identified risk the analysis stage can move on to attempting to determine the size or seriousness of each risk. Often this may mean determining the size or seriousness of the risk in relative terms to other risks. This can be done by using different techniques, for example:

- If doing this holistically, those involved in the risk analysis might collectively rank or categorise each of the identified risks in terms of their degree and relative importance.
- More formal analytical techniques can involve identifying the nature and extent of the consequences of each risk along with the likelihood that the risk may materialise and combining those results to determine a level of risk, which is often presented through the use of a matrix. The actual processes used to identify consequences and determine likelihood can also vary: Some countries may choose to employ more formal techniques such as surveys of experts or statistical analysis of the frequency of past ML or TF risk related activity. Others may choose to rely on the conclusions of a group discussion or workshop to help develop this information.

Understanding the consequences associated with ML and TF

54. In the process of analysing ML and TF risks, it is crucial to have a general understanding of why ML and TF occur. The acts of laundering money and financing terrorism are done to facilitate crime and terrorism more broadly. Profit is fundamental to the goals of most crime and therefore criminals make great efforts to move illegally obtained money and other assets in order to convert, conceal or disguise the true nature and source of these funds. In order for terrorists to carry out

their operations, attacks or maintain an infrastructure of organisation support, the need to have the ability to collect, receive and move funds. The availability of working capital is also fundamental for both criminals and terrorists to sustain their networks.

55. It is equally important to understand the consequences associated with the activity described above. This will assist in reaching conclusions about the relative importance of each identified risk. The consequences of this illicit financial activity are often viewed at the national or international level but also affect the regional, local and individual levels. Both *impacts* and *harms* (which make up consequences) can be further categorised into types, such as physical, social, environmental, economic and structural[23]. From a national perspective, one of the main consequences of ML and TF is that it has a negative effect on the transparency, good governance and the accountability of public and private institutions. ML and TF activity also causes damage to a country's national security and reputation and has both direct and indirect impact on a nation's economy. Box 1 sets out examples of consequences of money laundering, to assist those carrying out ML/TF risk assessments to reach conclusions about the relative importance of each identified risk.

Box 1. **Examples of Consequences of Money Laundering**

- Losses to the victims and gains to the perpetrator
- Distortion of consumption
- Distortion of investment and savings
- Artificial increase in prices
- Unfair competition
- Changes in imports and exports
- Effects growth rates
- Effects on output, income and employment
- Lower public sector revenues
- Threatens privatisation
- Changes demand for money, FX-rates and interest rates
- Increases in FX-rate and Interest rate volatility
- Greater availability of credit
- Higher capital in-flows
- Changes in foreign direct investment
- Risks for financial sector solvency and liquidity
- Profits for the financial sector
- Financial sector reputation
- Illegal business contaminates legal
- Distorts economic statistics
- Corruption and bribery
- Increases crime
- Undermines political institutions
- Undermines foreign policy goals
- Increases terrorism

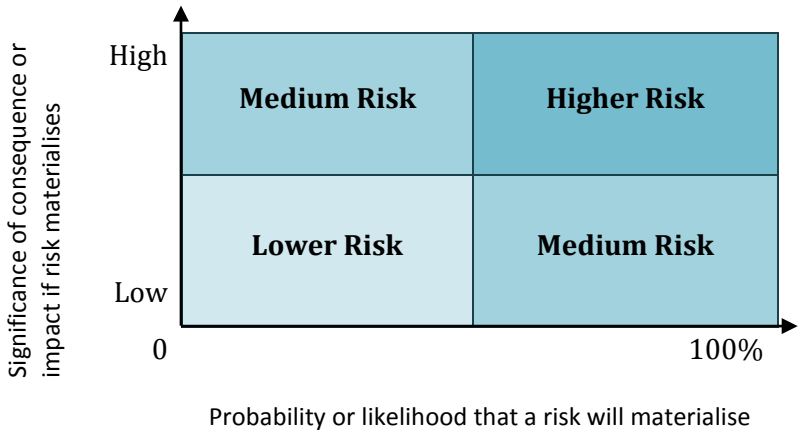
Source: Unger *et al*. (2006). The original source refers to *effects* – however, the term *consequences* as used in this table is consistent with the approach taken in this guidance.

56. A particular challenge especially when using more formal techniques is that ML/TF risks are inherently difficult to describe or measure in quantifiable or numerical terms. It is therefore important to remember that *risk* as we have discussed it in this guidance is a combination of threats, vulnerabilities along with consequences. If the level of risk of the individual risks can be examined according to their consequences or impact and the likelihood of their materialising, then a rough

[23] See FATF (2010), Annex C on "Crime and Terrorism Harm Framework".

estimate of risk level may be obtained. A very simple matrix as applied to a specific risk might be as shown in Figure 3.[24]

Figure 3. **Examples of a Risk Analysis Matrix**



4.3 Third stage: evaluation

57. The last stage of risk assessment is evaluation. 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. As indicated in the introduction, this guidance does not attempt to provide a full explanation of this step of the process. For the sake of completeness however, some general details are set out here.

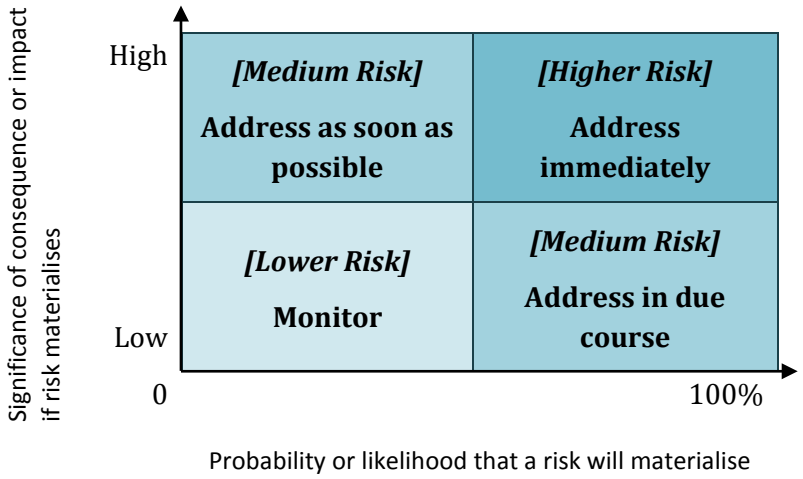
58. Depending on the source, there are a number of methods for addressing (or "controlling") risk, including prevention (or avoidance), mitigation (or reduction), acceptance or contingency planning. In the context of ML/TF risk and the risk-based approach, the most relevant of these methods are prevention (*e.g.*, prohibiting certain products, services, or activities) and risk mitigation (or reduction). The role of evaluating levels of ML/TF risk therefore normally leads to the development of a strategy for addressing the risks. Working from the example in the last section, the evaluation of risk levels for each of the analysed risks could result in courses of action as illustrated in Figure 4 [25], which is provided as a simple example of how the evaluation process might proceed at this stage:

---

24 This example is adapted from UNODC (2010). Note: This example is intended to give a general idea of the thought process at this stage and is not meant to prescribe a particular approach. In some cases, a more detailed matrix might be used in order to indicate a broader range of levels of risk. For example, probability of likelihood could use a 5-step descriptive scale such as *Very likely / Likely / Possible / Unlikely / Very unlikely, and impact or consequence might be described using a 3 point scale such as Major / Moderate / Minor.*

25 This example is adapted from UNODC (2010). See previous footnote.

Figure 4. **Examples of a Risk Evaluation Matrix**



59. According to this example, higher levels of risk might require more immediate action to mitigate it; lower levels of risk might require lesser action or some other response (the example here indicates monitoring). Alternatively, higher levels of risk may indicate systemic or deeply entrenched risks which require a broader response over time. By their nature, such responses generally require consultation (within government and between government and industry, among others), policy development and the implementation of measures, all of which can take time. The example shown here has been kept deliberately simple in order to clearly show the range of decisions that might be appropriate in addressing different levels of risk. A comprehensive ML/TF risk assessment process carried out at the national level might use a more detailed matrix in order to encompass a wider range of potential actions. Also note that, other types of risk matrices than the examples given above or a list ranking of the risks may also work, but the basic principles of the concept of risk as discussed in this paper should be applied.

60. The prioritisation of ML and TF risks at the evaluation stage will assist in the challenge of allocating scarce resources to fund AML/CFT programmes and other public policy and safety efforts. In the budgeting process, it is important to identify and prioritise issues that require attention. The evaluation process helps the authorities make decisions about how best to utilise resources and set priorities for regulatory agencies and the criminal justice system.

61. From an AML/CFT context, countries should implement necessary measures (for example, the FATF standards) and allocate appropriate resources to mitigate the risks which they have identified. In fact, the risk-based approach allows countries to develop a more flexible set of measures in order to target their resources more effectively, including by applying preventive measures flexibly to the financial and other sectors. Based on the risks identified, measures should address how best to prevent the proceeds of crime and funds in support of terrorism from entering into these sectors. Measures to mitigate risk should also address the ways in which these actors can better detect and report this activity. From an operational and criminal justice perspective, measures should be in place to better detect, disrupt and punish those who are involved in this activity.

5. OUTCOME OF RISK ASSESSMENTS

62. The actual results of a risk assessment can take different forms. For the public authorities that are ultimately the main users of the assessment, there is often an expectation that some form of a written report will be produced, although this is not strictly speaking a requirement of Recommendation 1[26]. If the assessment will be presented in report form, decisions on how it will be organised – along with the level of detail – are most usefully made early on the risk assessment process and normally relate directly to the purpose and scope of the assessment. For example, a ML/TF risk assessment with law enforcement or other operational services as the primary users might discuss risks according to the threats (actors and activities) that were the starting point of the assessment. For a report whose primary audience consists of regulators or the private sector, a discussion of the risks grouped according to vulnerability (sector, product, etc.) might be most useful.

63. Regardless of the form and presentation of the ML/TF risk assessment, it should ultimately allow public authorities to make a judgment on the levels of the risks and priorities for mitigating those risks. The policy response can then be made commensurate to the nature and level of the risks identified. It is therefore advisable that the risk assessment contain sufficient information about the source, nature, and extent of each risk to help indicate appropriate measures to mitigate the risk. Thus, the results of national ML/TF risk assessments can provide valuable input in the formulation or calibration of national AML/CFT policies and action plans. This policy decisions may ultimately affect a number of competent authorities and how they carry out their responsibilities (*e.g.*, how financial investigations are conducted). The results of ML/TF risk assessments may also help inform planning for technical assistance on AML/CFT matters by a broad range of donors and technical assistance providers.

Dissemination of assessments outcome

64. Once completed, authorities will have to consider how broadly the results of the risk assessment are to be disseminated amongst the various stakeholders. More specifically, Recommendation 1 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

65. Some ML/TF risk assessments may be considered to contain too much sensitive information to disclose publicly or that they may draw too much attention to the shortcomings in the AML/CFT system of a country. Furthermore, some of the information shared during the course of the assessment could be subject to confidentiality requirements. Nonetheless, appropriate information from assessments should be made available to the private sector to assist it in addressing the current ML/TF risks and new and emerging threats. In certain countries, committees or working groups with vetted private sector representatives have been created to share and discuss risk

[26] Countries will, however, be expected to demonstrate the process, mechanism and information sources used, as well as their understanding of and how they are addressing the identified risks.

assessment information. More generally, it may be helpful to share information – at a minimum – on the main factors considered and the conclusions of the risk assessment process with the private sector. Where the sensitive nature of the information prevents the broad distribution of the full results from the risk assessment report, consideration can be given to circulating sanitised information or summaries, or at least providing information on the methodology used, the findings and the conclusions. This approach could, for example, apply to information provided to assessors in the context of an AML/CFT assessment.

66. A particular objective of a ML/TF risk assessment could be to provide information to the public in order to enhance the general understanding of government AML/CFT initiatives. A typical output of a national ML/TF risk assessment is generally a public document. One challenge to overcome is that some information within the national assessment may be derived from classified or law enforcement sensitive sources. As such, some countries produce a non-classified version for the public.

ANNEX I. ML/TF RISK FACTORS RELATING TO THREAT

As mentioned in the Guidance, 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.

The following is a list of crime categories that may be useful in building a picture or estimate of ML/TF threats. This list is not exhaustive, and the individual categories should be viewed as examples and may be complemented in accordance with the purpose and scope of the assessment.

Consideration of all stages of ML

- Placement
- Layering
- Integration

Consideration of all stages of TF

- Raising / collecting funds
- Moving funds
- Using funds

Threat Factors[27]

- Nature and extent of relevant domestic criminal activity (*i.e.*, predicate offences).
- Types of predicate offences.
- Amounts of proceeds of crime generated domestically.
- Physical cross-border in and outflows of proceeds of crime.
- Amounts of proceeds of crime generated abroad and laundered domestically.
- Sources, location, and concentration of criminal activity, including within illegal underground areas in the economy.
- Nature and extent of relevant domestic terrorist activity and terrorist groups.

27 See section on the following page for a list of categories of proceeds of crime / criminal offences that may be useful in looking at threat factors.

- Nature and extent of terrorist activities and groups in neighbouring countries, regions, or sub-regions.

The following is a list of criminal activities organised into categories and sub-categories that may also be useful in building a picture or estimate of threat (in the proceeds of crime environment). This list is not exhaustive, and the individual categories and subcategories should be viewed as examples.

Predicate Crime Categories for ML Crime Categories and Sub-Categories [Source: IMF]

Participation in an organised criminal group & racketeering

- Sophisticated organisations (*e.g.*, mafia, yakuza)
- Drug organisations
- Motorcycle gangs
- Street gangs
- Other

Terrorism and terrorist financing

- Raising funds from criminal activities
- Raising funds from "legal" or apparently lawful activities
    - Willing Donors using "Legal" Fundraising (*e.g.*, NPOs)
    - Deceptive Use of "Legal" Fundraising (*e.g.*, NPOs, donors unaware of TF use)
    - Donated from legal income (*e.g.*, salaries & profits)
- Other

Trafficking in human beings and migrant smuggling

- Trafficking (involuntary)
    - Inwards
    - Outwards
- Migrant smuggling (voluntary)
    - Inwards
    - Outwards
- Other

Sexual exploitation, including sexual exploitation of children

- General - unclassified
- Illegal prostitution
- Sexual slavery
- Procuring sexual activity with minors

- Selling/distributing illegal pornographic material
- Selling/distributing illegal pornographic material involving minors
- Other

Illicit trafficking in narcotic drugs and psychotropic substances

- Cocaine
- Marijuana/Cannabis
- LSD
- Ecstasy
- Meth/Amphetamines
- Heroin/Morphine/Opium
- "Magic" mushrooms
- Other

Illicit arms trafficking

- Small arms/guns
- Light weapons
- Larger Military hardware
- Ammunition
- Weapons of mass destruction
- Other

Illicit trafficking in stolen and other goods

- Stolen goods (NB: only to extent not captured under *e.g.,* theft)
- Gems
- Precious metals
- Radioactive materials
- Cultural goods
- Other

Corruption and bribery

- Bribery - major
    - Friendly GST/tax assessments
    - Avoiding investigation/prosecution
    - Procurement contracts
    - Permits/permissions/licenses
    - Other
- Graft - minor
    - Police
    - Traffic Police

    - Customs Officers
    - Licensing/Permit officials
    - Other
- Embezzlement/misappropriation (theft)
    - Central/federal government
    - Local/state/county etc. government
- Bribery of private sector
- Bribery of foreign officials
- Bribery or embezzlement - international organisations
- Illegal lobbying and political campaign financing
- Other

Fraud

- Against government - General
- Against government - VAT/GST fraud
- Embezzlement/misappropriation (excluding from government by officials)
- Lending fraud (*e.g.*, mortgage fraud)
- Payment instrument fraud (*e.g.*, credit card, check fraud)
- Insurance fraud
- Healthcare fraud
- Benefit fraud
- Vendor, supplier & procurement fraud
- Confidence tricks/scams
- False billing/invoicing
- Cyber & Internet selling frauds (*e.g.*, "phishing")
- Investment frauds (*e.g.*, Ponzi & pyramid schemes)
- Other fraud

Counterfeiting currency

- Local currency
- Foreign currency
- Other

Counterfeiting and piracy of products

- Illegal parallel imported products
- Patents/copyright/trademark infringement
- Clothing and shoes
- Accessories: bags/sunglasses/watches etc.
- Books

- Information technology
- CDs/DVDs, etc.
- Cigarettes
- Foodstuffs
- White ware & other electricals
- Pharmaceuticals
- Of collectibles (*e.g.,* wine, antiquities)
- Software
- Other

Environmental crime

- Illegal fishing
- Illegal logging
- Illegal dumping/polluting
- Illegal mining
- Other illegal extraction
- Illegal trading in endangered species (CITES)
- Illegal construction
- Other

Murder, grievous bodily injury

- Murder - for hire/contract killing
- Murder - motive is profit (*e.g.,* insurance claim)
- Grievous bodily injury- for hire or to derive funds or assets
- Other

Kidnapping, illegal restraint, and hostage taking

- Kidnapping/abduction for profit
- Hostage taking for ransoms
- Other

Robbery or theft

- Burglary - commercial
- Burglary - domestic/residential
- Theft/stealing/larceny
- Theft of motor vehicles (including car-jacking)
- Theft from motor vehicles
- Shoplifting
- Pick pocketing
- Bank robbery

- Pilfering/embezzlement (theft by employee)
- Robbery/mugging (including armed robbery)
- Cyber theft (*e.g.*, transferring bank balances through illegal account access)
- Other

Smuggling

- Prohibited imports
- Cigarettes
- Alcohol
- Cash smuggling of "clean" money (including dirty money would be double counting)
- Foodstuffs
- Prohibited exports
- Fuel
- Other

Extortion

- Blackmail
- Protection money/rackets
- Other

Forgery

- Of financial assets
- Philatelic forgery
- Of other documents
- Fake passports
- Fake ID/driver licenses
- Of art
- Other

Piracy (i.e., maritime)

- Theft from piracy
- Extortion or ransoms from piracy
- Other

Insider trading and market manipulation

- Insider trading
- Traded markets - market manipulation
- Anti-trust/cartel or anti-competition violations
- Boiler room scams
- Other

Tax & excise evasion

- Personal income tax
- Withholding tax
- Corporate income tax
- On illegal income sources
- Sales/turnover tax, VAT
- Customs/excise under invoicing - exports
- Customs/excise under invoicing - imports
- Customs/excise false declaration of quantity & product
- Sprits, tobacco, fuel excise evasions
- Gaming machine taxes and excise evasions
- Excise evasions related to counterfeit and piracy of products
- Other excise evasions
- Departure taxes & fees
- Death & estate duties
- Stamp Duty
- Capital gains taxes
- Real estate rental etc. taxes
- Informal sector
- Illegal transfer pricing
- Other

Illegal gambling

- Illegal lottery
- Illegal betting/bookmaking
- Illegal gambling houses/casinos
- Illegal online gambling
- Other

Money laundering

- Of foreign proceeds of crime

Other Proceeds Generating Crimes

- Computer crime
- Illegal trading of goods and services
    - Alcohol and tobacco
    - Pharmaceuticals, including internet pharmacy
    - Anabolic steroids
    - Party and other "non-narcotic" drugs

- Antiquities

- Illegal carrying out of a regulated/licensed business
  - Loan sharking/illegal lending
  - Illegal remittance activity
  - Illegal/prohibited FX dealing or money changing
  - Other illegal/prohibited financial services
  - Illegal professional services (*e.g.*, accounting, legal etc.)
  - Illegal health related services (*e.g.*, abortions, dentistry, donor tissue operations and trading etc.)

ANNEX II. ML/TFRISK FACTORS RELATED TO VULNERABILITIES

In order to understand the ML/TF risks facing a country, the relevant vulnerabilities need to be identified. This annex contains a longer list of examples of factors that may be considered at this stage of the ML/TF risk assessment to help identify relevant vulnerabilities. They have been generally arranged according to the analytical framework known as "PESTEL" (an acronym based on the first letters of the major categories: political, economic, social technological, environmental and legislative). This list is neither exhaustive nor binding, nor would these factors apply in every country's ML/TF risk assessment and they should be applied in the context of each country[28].

Political factors

- Structure of the political system
- Stability of the present government
- Level of political commitment for AML/CFT programmes
- Level of political commitment to fighting crime
- Unaddressed history of terrorism financing activity
- Prevalence of organised crime, especially if involved in illicit drug production, illicit drug trafficking, kidnapping for ransom, extortion, intellectual property crime
- Presence of illicit small arms trade
- Prevalence of smuggling networks
- Presence of individuals, groups or organisations that support or promote violent extremism
- Weak government reach in some areas of the country, particularly border areas; porous borders
- High levels of corruption
- Adequacy of human, financial, and other resources of competent authorities
    - Inadequate resources
    - ML/TF not a national priority
    - No ML/TF risk assessment conducted by the authorities
    - Reluctance to acknowledge ML/TF risk
    - Lack of specialised training
    - Lack of commitment of financial sector, including low levels of reporting and/or lack of quality of STRs

28 Some of the examples are taken from UNODC (2010).

- Financial sector not sufficiently concerned or incentivised regarding vulnerability to ML-related reputational risk
- Requirements of AML/CFT regime not well understood or implemented by financial institutions and DNFBPs
- Inadequate resources allocated to regulation of NPOs, given the risk level identified
- Inadequate resources allocated to address the issues on identify beneficial owners of foundations, associations and other similar entities, such as trusts

- Effectiveness of operations of competent authorities
  - Authorities' capabilities to suppress crime generally, and predicate offences to ML/TF specifically
  - Systemic weaknesses in law enforcement, and in authorities' efforts to counter crime generally, in particular ML/TF
  - Limited or non-existent ability of intelligence and law enforcement engaged in combating ML or TF to use financial information in their investigations
  - Inadequate co-ordination and information-sharing among law enforcement and intelligence agencies involved in combating ML/TF
  - Inadequate co-ordination among national authorities involved in combating ML/TF
  - Significant differences in procedure among competent authorities responsible for combating ML/TF
  - Lack of capabilities of financial intelligence unit (FIU) to process the reports that it receives
  - Lack of capabilities of law enforcement authorities (LEAs) to suppress ML or TF, which might result in ML or TF not being detected or investigated adequately
  - Lack of inter-agency cooperation that impedes AML/CFT processes and operations
  - Lack of capabilities of the prosecutors, the judiciary, and the prison system to deal with ML or TF related crimes, including weaknesses in the law, and other weaknesses that mean that offenders are not prosecuted, convicted, or sanctioned adequately or deprived of their assets or funds
  - Weaknesses in the authorities' ability to gather and share information due to a lack of capacity or legal privilege

- Inability to obtain convictions for ML/TF and related offences
- Lack of an operational FIU or FIU ineffective; inability or lack of capacity to examine STRs
- Lack of engagement or reluctance to engage regionally or internationally on AML/CFT issues, including on requests for assistance
- Ineffective border controls
- Border and immigration officials lack access to INTERPOL I-24/7 global police communication system
- Weak cash courier control at border points
- Weak AML/CFT oversight
- Government does not conduct regular reviews of terrorism financing risk in its NPO sector

Economic factors

- The type of economic system
- The amount of regulation within the economy
- Average earnings of the population
- Currency exchange rates
- Cost of services
- Size of the financial services industry
- Large, complex economy, or both (perhaps making it easier for ML/TF operations to go unnoticed)
- General opacity of the financial system
- Composition of the financial services industry[29]
    - Products, services, and transactions
        - basic information on sectors or products
        - existence of those that facilitate speedy or anonymous transactions
        - cash transactions and cross-border funds transfers
        - delivery channels
        - existence of high-risk correspondent relationships between banks

[29] See also the list of financial institutions and services in later in this Annex.

        - existence of measures to facilitate fiscal optimisation by non-residents (tax haven)
    - Customer
        - types and ranges of customers (*i.e.,* entities, persons, etc.)
        - nature of business relationships
        - existence of higher risk customers
        - adherence to regulatory provisions applicable to customers
        - adherence to any restrictions on customer transactions
    - Geographic
        - business and customer base in specific geographic areas
        - non-residents
        - customers from geographic area of concerns
        - adherence to any requirements in other countries
        - trans-national or cross-border movements of funds
- Ownership/ control of financial institutions and requirements concerning the identification of beneficial owners that are non-residents
- Corporate governance arrangements in financial institutions and the wider economy
- Nature and role of legal persons and legal arrangements in the economy
- Nature, existence, and size of sectors for legal persons and legal arrangements
- Nature of payment systems and the prevalence of cash-based transactions
- Cash-based economy with large informal sector; high percentage of cash outside legitimate banking system, especially relative to comparable countries
- Strict application of financial institution secrecy and other secrecy – including professional secrecy
- Geographical spread of financial industry's operations and customers
- Economic ties with jurisdictions at high risk of experiencing terrorism, political instability, or both
- Presence of NPOs active in overseas conflict zones or in countries or regions known to have a concentration of terrorist activity

- Presence of NPOs raising funds for recipients in a third country which are part of an organisational structure that engages in violent or paramilitary activities
- Opaque relations between grantees and NPOs disbursing funds or resources to grantees, *e.g.,* grantees are not required to disclose to the NPO how funds are used; no written grant agreement; NPO does not perform grantee due diligence, or due diligence is random and inconsistent; NPOs may disburse large sums for unspecified projects selected by the grantee.
- Effectiveness of financial institutions and DNFBPs in implementing the AML/CFT obligations or control measures
    - Customer due diligence
    - Ongoing due diligence, including transaction monitoring
    - Reporting measures currently performed
    - Internal controls
    - Record-keeping

Social factors

- The demographics of the society
- Extent of social inclusiveness
- Significant population shifts
- The ethnic diversity of the population
- Cultural factors, and the nature of civil society
- Areas of social, ethnic or political conflict
- Cultural immigrant, emigrant or religious ties with jurisdictions at high risk of experiencing terrorism, political instability, or both
- Low level of consultation / co-operation between government and financial sector
- Affiliates of banks circumvent international prohibitions that screen transactions for terrorists, drug traffickers, rogue jurisdictions and other wrongdoers
- Bank personnel not required to routinely share information among affiliates to strengthen coordination
- Requirements of AML/CFT regime not well understood or implemented by financial institutions and DNFBPs

Technological factors

- Use of transportation
- New communication methods

- The use of technology in money transfer
- Introduction and use of new payment methods

Environmental and geographical factors[30]

- Global environmental factors such as availability of water, global warming, etc.
- The use and re-use of resources
- Impact of the local environment on crime such as housing, security etc.
- Impact of environmental legislation

Legislative factors

- Criminal justice system and legal environment
- Ease with which new legislation can be passed
- Review process for current legislation
- Impact of international standards on national legislation
- Strengths and weaknesses in legislation combating serious and organised crime
- Strengths and weaknesses in current AML/CFT legislation
    - AML/CFT preventive controls, including AML/CFT specific supervision and monitoring, that collectively do not deter ML or TF nor result in it being detected if it does occur
    - AML/CFT cross-border controls and international cooperation
    - Jurisdiction not a party to the International Convention for the Suppression of the Financing of Terrorism, the United Nations Convention against Transnational Organised Crime and its Protocols, and/or the United Nations Convention against Corruption
    - Adherence to international standards or conventions applicable to the specific sector or product
    - ML/TF not criminalised or inadequately criminalised
    - Incomplete coverage of predicate offences to ML
    - ML/TF not criminalised as a standalone offence
    - TF not a predicate offence to ML offence
    - TF not criminalised unless linked to a specific terrorist act
    - TF only criminalised in relation to the treaty-based offences

30 Certain major categories provided in this example may not be relevant in all ML/TF assessments.

- No measures or inadequate measures to freeze without delay terrorist funds and assets
- Freezing of terrorist funds does not extend to other terrorist assets
- No legislation denying safe haven to those who assist or commit terrorist acts (laws on modalities of inter-State cooperation, extradition, mutual legal assistance, transfer of criminal proceedings, etc.)
- Government has not reviewed its own policies, legislation and other tools in respect of terrorism financing risk in the NPO sector and taken steps to address shortfalls
- Regulation of charitable donations does not cover overseas donations
- Lack of early warning arrangements with other jurisdictions on CFT
- Financial sector not prohibited from conducting relationships with shell banks or shell companies
- Adequacy of AML controls
    - Customer due diligence
    - Ongoing due diligence including transaction monitoring
    - Reporting measures currently performed
    - Internal controls
    - Record keeping
    - Lack of regulation on beneficial ownership
- Lack of guidance to relevant authorities on beneficial ownership
- Limited or absence of risk-based approach guidance on AML/CFT provided by regulatory, oversight and supervisory authorities
- Limited regulation of money or value transfer systems
- Entities not registered and size of sector unknown
- No system of registering or licensing service providers; difficult to take enforcement action and thereby to formalise flows of funds

- Any non AML/CFT controls that apply to entities that can be abused for ML or TF, including general supervision or monitoring
- Any non-AML/CFT related cross-border controls, including general border security
- Extent and efficacy of compliance audits
- Enforceability of rules or guidance
- Existence of a regulator or supervisor
- Links with other financial intermediaries
- Legal or other constraints on products, services, transactions
- Coverage or requirements in other countries

The following table provides a generic list of entities /sectors that may be useful in building a list of the ML/TF vulnerabilities that can be exploited in regulated entities. In particular, it may be worth using such a list to think about vulnerabilities in the context of types of products and services offered by each type of institution or firm and the adequacy of their AML/CFT controls. This list is not exhaustive, and the individual sectors / entities included here should be viewed as examples.

Table 1. **Institution and firm categories by sectors**

Sector	Categories of institutions and firms
Banks and credit institutions	*All banks or commercial banks (including: foreign banks, government-owned banks, merchant banks, special purpose banks)*
	All offshore banks (offering services exclusively to non-residents)
	Building societies, cooperatives and credit unions
	Central bank WITHOUT retail base
	Central bank WITH retail base
	Finance companies
	Savings institutions (including postal savings service)
	Microfinance deposit takers
	Merchant banks
	Shell banks
Securities industry	*Advisers*
	Fund and asset managers (including mutual funds)
	Futures (including commodities) & derivatives brokers and dealers
	Markets, registries & exchanges
	Securities firms (brokers, dealers and other companies)
	Superannuation and pension companies

Sector	Categories of institutions and firms
	Other
Insurance industry	*Life insurance agents and brokers*
	Non-life insurance agents and brokers
	Non-life insurance companies
	Offshore insurers
	Superannuation and pension companies
	Other Insurance
Money services businesses (MSBs)	*Card issuers/E-payment (credit, debit, E-cash/money etc.)*
	Check issuers and cashers
	Foreign exchange dealers (including bureaux de change and money changers)
	Money remitters and transfer agents (including any postal service that offers this service)
	Undertaking of bill payment business
	All (Other) MSBs
Other financial institutions	*Hire purchase companies*
	Mortgage providers
	Other lenders
	Other specialist financial institutions (such as development FIs)
	Pawnshops (if they "lend")
	Providers of deposit boxes
	Specialised financial institutions
	Cash handling firms
DNFBPs	*Accountants*
	Auditors
	Casinos
	Dealers in precious metals and stones
	Lawyers (including barristers, solicitors, and other legal professionals)
	Notaries
	Real estate agents (including licensed conveyancers)
	Trust and company service providers (including: company formation agents)
	All (Other) DNFBPs

Sector	Categories of institutions and firms
Other entities	*Advisors, including tax and financial*
	Bookmakers, betting, gaming & lotteries
	Motor vehicle retailers
	Boat charterers, sellers, and re-sellers
	Aircraft charterers, sellers, and re-sellers
	Art and antique dealers
	Auction houses
	Other dealers and traders in high value goods
	Pawnshops
	Travel Agents
	Convenience, grocery, liquor stores
	Laundromats, car washes, parking businesses
	Other cash intensive businesses
	Construction companies
	Customs agencies and brokers
	Mail and courier companies
	Hotels
	Restaurants and bars
	Mining, logging, and other extractive industry companies
	Other
Legal persons	*Bodies corporate*
	*Registered companies **
	*Public companies **
	*Companies that have issued bearer shares **
	*Companies owned or controlled by non-residents **
	*International or (foreign) business companies or corporations **
	*Other types of company **
	Foundations
	Anstalt
	Partnerships
	Associations
	Similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property
	All legal persons (other than companies) that are owned or controlled by non-residents including branches or offices of foreign legal persons authorised to operate in the

Sector	Categories of institutions and firms
	*jurisdiction **
Legal arrangements	*Express trusts (i.e., with a written deed of trust)*
	Fiducie
	Treuhand
	Fideicomiso
	Other similar legal arrangements
	*International Trusts**
	*All legal arrangements established or controlled by non-residents**
Non-profit organisations (NPOs)	*NPOs - registered or licensed*
	NPOs - not registered or licensed
	*All NPOs established or controlled by non-residents**

Table note
* These are memorandum items only as they should already appear in other categories.

ANNEX III. EXAMPLES OF NATIONAL-LEVEL ASSESSMENTS

This annex shares countries' efforts to assess ML/FT risks at the national level (whether focusing on threats, vulnerabilities, or both). These are presented as examples only. At the time of the publication of this guidance, the individual efforts had not been assessed for compliance with Recommendation 1; therefore, their presentation here should not be considered as an endorsement by FATF.

Australia

FATF Guidance on risk assessments – project group

Australian National Threat Assessment on Money Laundering 2011 (NTA)

Australia adopted a 'top-down' approach in 2011, producing the country's first National Threat Assessment (NTA). The NTA was a key element of the organised crime strategic framework the Australian Government adopted in 2009. The NTA involved only government agencies. AUSTRAC, the national FIU and AML/CFT regulator (*i.e.,* supervisor), led the project with primary input coming from five national government agencies (policy, revenue, law enforcement and border protection) and one state-based law enforcement intelligence agency. Incidental information came from a handful of national and state agencies on particular issues as required.

A two-tiered system was established to coordinate input and provide direction across agencies. A steering committee of senior officials was formed to provide guidance and governance to the assessment and resolve any issues that arose. The level below involved a working group of intelligence analysts, law enforcement officers and policy advisers to collect and analyse information, and work with the FIU on drafting the assessment. Once approved by the steering committee and the head of the FIU, the assessment was submitted to the heads of operational agencies in national government (comprising law enforcement, the FIU, border protection and regulatory agencies).

The NTA draws together information from across key government agencies to form a consolidated picture of the Australian money laundering environment. It is focused on the Australian environment and what Australian agencies and experts see as the current and emerging threats. Close attention is paid to money laundering associated with higher risk organised crime activity. It also examines high-risk countries that influence the Australian environment. International experience is drawn upon where required to amplify an aspect of the Australian situation, or to help address gaps in the Australian picture.

Information sources are primarily intelligence based. Current intelligence insights, operational cases, and expert views inform the discussion of current and projected money laundering activity. Limited statistical data, particularly the financial value tied to money laundering activity, meant the NTA is largely a qualitative threat assessment.

Threat matrix

The NTA modified the 'features' adopted in the FATF *Global Money Laundering and Terrorist Financing Threat Assessment* (GTA)[31], using terminology about channels, sectors and vulnerable individuals (industry insiders and PEPS) that would be readily understood by an Australian audience. Assessment of each area took into account:

- Government measures (law and regulation, law enforcement and regulatory activity, specialist intelligence work where relevant)
- Current intelligence picture
- Drivers and enablers (adopted from the GTA)
- Gaps in intelligence, information and measures
- Threat assessment with a three-year forecast where possible

To overcome the limitations faced in trying to apply conventional threat analysis (intent x capability = threat) to money laundering, a threat matrix (see Table 2 below) was customised for Australia's circumstances to rank relative levels of threat. It assessed threats and vulnerabilities in terms of:

- **Accessibility** or availability of services that might be misused for ML – scale from easy, moderate to difficult (the easier to access, the higher the threat)
- **Ease of use** – same scale as above
- **Deterrence** – scale of significant, limited to weaker (significant = measures reasonably effective at lowering threat of ML)
- **Detection** – scale of likely (detection of ML), limited to difficult (detection is unlikely due to intelligence gaps, opaque and complex services)
- **Criminal intent** to launder (a function of the above categories and assessments of current and emerging organised crime behaviour and trends)

Weightings for the scales used above were developed to produce rough scores of levels of threat, from undetermined to low, through to medium and high. Scoring was not adopted as a strict science, but rather as a starting point to stimulate expert discussion among the involved agencies. Threat scores were also used in conjunction with the analysis of each area, to test intelligence judgements and, vice versa, test the validity of the scoring system itself.

[31] FATF (2010).

Table 2. **Australian Threat Matrix**

Threat factors	Low threat	Medium threat	High threat
ACCESSIBILITY ***e.g.* accessibility and relative cost**	**Difficult** Difficult to access and/or may cost more than other options.	**Moderate** Reasonably accessible and/or a financially viable option.	**Easy** Widely accessible and available via a number of means and/or relatively low-cost.
EASE OF USE ***e.g.* knowledge and/or technical expertise and support required**	**Difficult** Requires more planning, knowledge and/or technical expertise than other options.	**Moderate** Requires moderate levels of planning, knowledge and/or technical expertise.	**Easy** Relatively easy to abuse; little planning, knowledge and/or technical expertise required compared to other options.
DETERRENCE ***e.g.* existence of AML and/or other barriers to abuse**	**Significant** Deterrence measures and controls exist and are reasonably effective at deterring money laundering.	**Limited** Deterrence measures and controls have some effect in deterring criminal abuse of the service.	**Weaker** There are limited or no measures and controls in place, or they are not working as intended.
DETECTION ***e.g.* ability for money laundering to be identified and reported to authorities**	**Likely** A range of money laundering methods is visible and likely to be detected.	**Limited** Some money laundering methods may be visible but limited reporting, high volumes of funds flows and/or effective evasion techniques limits detection.	**Difficult** Detection is difficult and there are few financial or other indicators of suspicious activity.
INTENT ***e.g.* perceived attractiveness of money laundering through this mechanism**	**Low** Perceived as relatively unattractive and/or insecure.	**Moderate** Perceived as moderately attractive and/or fairly secure.	**High** Perceived as attractive and/or secure.

High-risk countries[32]

To improve the capacity of Australian authorities to assess and weigh-up the ML threats/risks foreign countries pose to Australia, the NTA developed a high-risk country matrix. It essentially is a checklist of the main indicators and attributes which influence a country's risk profile, as a source, destination or conduit for laundered funds. A copy of the matrix table, sanitised with countries removed, is attached to this paper. It involved a larger set of indicators (listed below) than the

32 Even though the NTA is a threat assessment, the term 'high-risk countries' was used due to its commonplace usage in official circles.

threat matrix above. Many of the risk indicators are drawn from FATF guidance. Numerical weightings or scoring were not used with the matrix, but the format lends itself to such an approach if required.

For the sake of clarity, the NTA divided high-risk countries into two broad crime types: organised/transnational crime and offshore tax evasion. Although the boundary between these two categories is blurred and some countries appear in both groups, this approach helped to sift through a long list of countries. It also provided a sharper focus on the nature of illicit funds flows involving different countries, than would have been the case if they had all been lumped under the 'high-risk' tag.

High-risk country indicators

- Variable regulations, such as lax AML/CFT provisions, weak regulation of business registration, financial markets and foreign currency exchange
- Preferential tax regimes identified by the OECD
- Strong secrecy provisions in banking and finance
- High volume of non-bank international remittances
- Regional or global financial centres
- Free-trade or special economic zones
- Source countries for illicit commodities and services
- Transit countries for illicit commodities and services
- Low tax on foreign income
- Ability to easily create complex legal entities to hide beneficial ownership of assets
- Countries with perceived high-level corruption
- Countries embroiled in high-level internal or external conflict
- Patterns of evasion of exchange controls by legitimate businesses
- Limited asset forfeiture and seizure powers
- Weak law enforcement and border control capabilities
- Large parallel or black market economies
- Cash intensive economies
- Countries with no extradition treaty with Australia
- Jurisdictions that are either a place of residence for members of a criminal network or where members of a criminal network have strong familial or cultural ties, or both
- Jurisdictions where criminal entities can obtain dual nationality

Approach and lessons learnt

Since it was Australia's first NTA, the intention was to involve a core of key government agencies in laying the foundations upon which subsequent national assessments could build. Wider involvement from industry and other government bodies at the national and state/territory level is something to be considered for future assessments.

A key lesson from the first NTA is that any decision to involve more partners or stakeholders should be made on the basis of the value of data, intelligence and expertise they can commit to an assessment. Relevant expertise and a guaranteed commitment of resources (staff and time) are essential for the successful completion of such a large exercise. The 'hidden cost' in time and staff in consulting and coordinating many stakeholders should not be underestimated.

The NTA examines only money laundering and excludes terrorism financing threats. Differences between ML and TF, limited cases in the Australian context and difficulties in managing highly sensitive intelligence were all seen as likely to create added problems for a complex assessment that was first of its kind in Australia and largely exploratory. As with the decision to limit the number of agencies involved, the NTA was seen as paving the way to undertake a TF assessment in the future.

The NTA originally included, in line with the GTA framework, harms analysis for each area under examination. Harms were later omitted to avoid any conceptual confusion as to whether the NTA was a *threat* assessment (harms or consequences excluded) or a *risk* assessment (harms and consequences included). The more important reason for the omission was due to the lack of available evidence of ML harms in Australia, beyond sustaining continued and expanded criminal activity. Overseas experience of ML harms was largely seen as not directly relevant or provable in the Australian context.

The Netherlands

In 2005, a study was conducted titled: "The Amounts and Effects of Money Laundering"[33]. Its objective was to obtain better information on the amount, flows and effects of money laundering. The study was based on a quantitative method to estimate the amounts, flows and effects of money laundering. In addition, (extensive literature) research was carried out on definitions, typologies and growth effects. There was also an effort to identify forms of money laundering, typically existent in The Netherlands. The findings were mainly based on qualitative judgments but sometimes supported by quantitative data. The results of the study were used as input for policy formulation.

In 2011 a National Threat Assessment (NTA) was carried out in the Netherlands. The Ministry of Finance was leading the project and established a project plan which was submitted to and approved by the Financial Expertise Centre[34]. The exercise commenced by interviewing all relevant stakeholders, including for example: financial sector, supervisory authorities, research institutes

[33] Unger *et al.* (2006).

[34] The Financial Expertise Centre (FEC) is a partnership between authorities that have supervisory, control, prosecution or investigation tasks in the financial sector and was founded to strengthen the integrity of the sector. Authorities involved in the FEC are: Dutch Central Bank, Financial Markets Authority, Public Prosecutor, Tax Authorities, Intelligence Services, National Police, Ministry of Justice and Ministry of Finance.

and law enforcement. Based on the outcome of these interviews, the project team identified a list of mayor topics/issues and organised several workshops to discuss the selected items. Participants in these workshops where policymakers, supervisory authorities, prosecutors, police and tax authorities. As a result of this series of workshops three mayor topics where identified and these became subject of an in depth research. The project team analysed and described cases and trends/developments on these items and made recommendations for further work on these issues. Finally, the report has been presented to the Ministry of Finance and the Ministry of Justice with the objective to translate the outcome of the NTA into national policy measures. Relevant information resulting from this process has been published or made available to relevant non-public bodies, but the NTA itself remained a classified document.

In 2012 the National Police Services Agency (KLPD) conducted a National Threat Overview focused on money laundering. The method used by the KLPD was the following: again the research was commenced by a series of interviews with stakeholders. These interviews served as a basis for an in depth research in criminal files and data systems. This resulted in a description of several methods of money laundering, characterisation of persons involved and consequences for the Dutch society. Finally, the National Threat Overview is addressing some general developments concerning money laundering in the future.

Switzerland: Example of a risk assessment used as the basis for applying low-risk exemptions

Switzerland has developed a risk assessment process as a basis for applying low risk exemptions. A working group was established from September 2009 to January 2010, which was composed of experts from the banking, insurance and non-banking sectors, auditors, law enforcement authorities and the financial regulator. The working group identified low-risk products for which the exemptions could apply. This work resulted in the adoption of regulation which establishes an ongoing risk assessment process.

On the basis of the aforementioned regulation, a committee of experts, established by FINMA, can authorise exemptions from CDD measures for customer relationships at the request of SROs or financial intermediaries if there is a proven low risk for money laundering. In order to get a decision from FINMA allowing a financial intermediary to benefit from an exemption, the requestor has to provide all elements necessary for FINMA to take this decision. FINMA then verifies if the regulatory conditions for an exemption are met, and in particular if the low risk is given on a case-by-case basis. To come to a decision, FINMA analyses every request separately and in detail. Different criteria are taken into consideration. FINMA examines whether the FATF has already considered the activity under the risk aspect. It examines if similar cases have already been subject to criminal or other enforcement measures. Finally, FINMA decides if the risk is low in the concrete case, but also if it will remain low if the circumstances would slightly change. Consideration is given to product, services, transactions as well as customer risk and to the legal environment, as well as to every other relevant characteristic of the activity, in order to decide whether the risk is low. FINMA has the legal obligation to publish its practice.

United States

In 2005, the United States initiated its first multi-agency money laundering threat assessment. Quantitative inputs included prosecution data from federal law enforcement agencies and suspicious transaction reporting via the financial intelligence unit. Qualitative inputs came from law enforcement and regulatory case studies with private sector reporting.

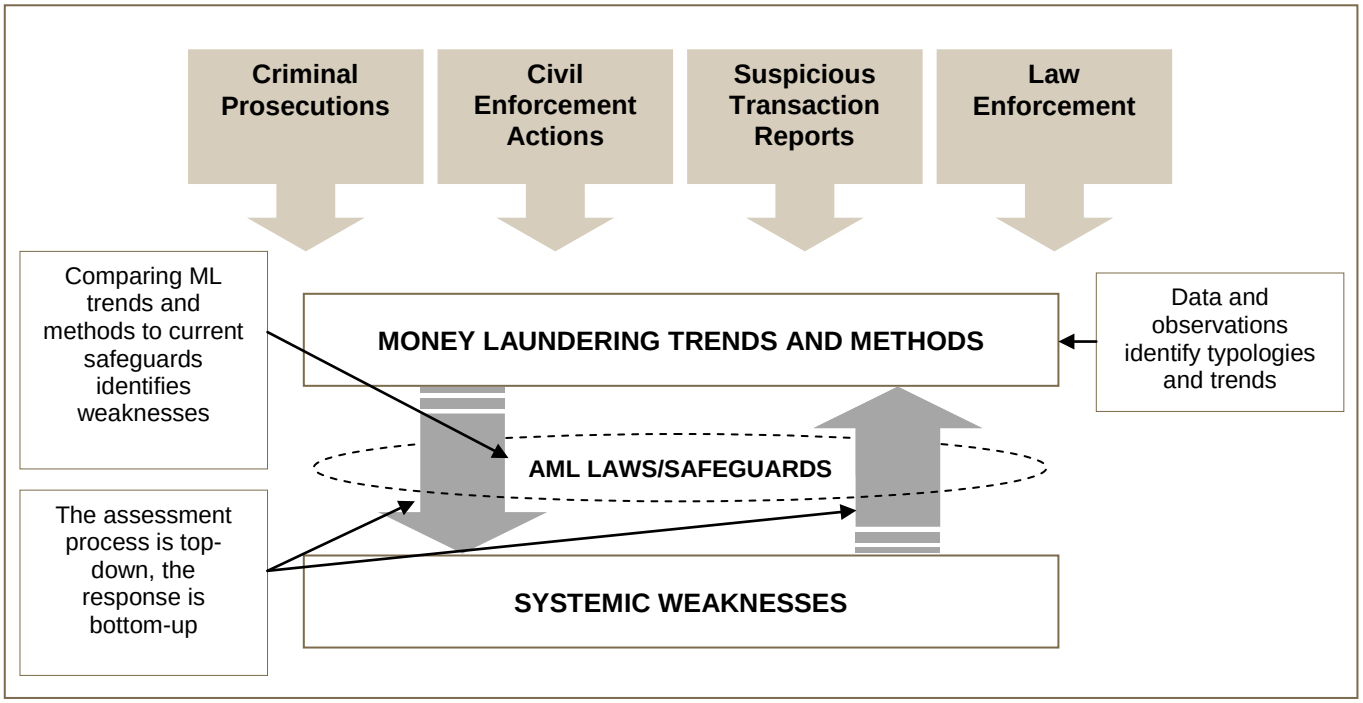
The 2005 *U.S. Money Laundering Threat Assessment*[35] was divided into the following sections: banking, money services businesses, (*i.e.*, money transmitters, cheque cashers, currency exchangers, money orders and stored value cards); online payment systems; informal value transfer systems; bulk cash smuggling; trade-based money laundering; insurance companies; shell companies and trusts; and casinos.

The project team made assumptions and observations about vulnerable sectors using the available information, considered whether adequate safeguards were in place to address the identified vulnerabilities and made a subjective determination about the residual threat.

This was a multi-agency process, including offices and agencies under the US Departments of Homeland Security, Justice and Treasury. Also participating was the Board of Governors of the Federal Reserve System and the United States Postal Inspection Service.

The available information was synthesised to form a qualitative assessment, which included, to the extent possible, the relative effectiveness of AML safeguards. In some cases, data was available to support subjective judgments regarding effectiveness (see Figure 5). Otherwise, the determinations were the result of broad intergovernmental discussion and analysis.

Figure 5. **Flow chart depicting US money laundering assessment and strategy formation process**



35 Money Laundering Threat Assessment Working Group (U.S. Department of the Treasury, *et al.*) (2005).

ANNEX IV. SPECIFIC RISK ASSESSMENT METHODOLOGIES

The International Monetary Fund Staffs' ML/FT National Risk Assessment Methodology:
www.fatf-gafi.org/media/fatf/documents/reports/Risk_Assessment_IMF.pdf

The World Bank Risk Assessment Methodology
www.fatf-gafi.org/media/fatf/documents/reports/Risk_Assessment_World_Bank.pdf

BIBLIOGRAPHY

Relevant FATF material (all available at: www.fatf-gafi.org)

FATF (2012), *The FATF Forty Recommendations*, FATF, Paris.

FATF (2010), *Global Money Laundering and Terrorist Financing Threat Assessment*, FATF, Paris.

FATF (2008), *Money Laundering and Terrorist Financing Risk Assessment Strategies*, FATF, Paris.

FATF, (2007), *Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*, FATF, Paris.

Country-level assessments of interest (available on line)

Australia:

AUSTRAC (2011), *Money laundering in Australia 2011*, Sydney, www.austrac.gov.au/files/money_laundering_in_australia_2011.pdf

Netherlands:

Unger *et al.* (2006), *The Amounts and the Effects of Money Laundering, Report for the Ministry of Finance*, Amsterdam, www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2006/02/16/onderzoeksrapport-the-amounts-and-the-effects-of-money-laundering/witwassen-in-nederland-onderzoek-naar-criminele-geldstromen.pdf

New Zealand:

New Zealand Police (2010), *National Risk Assessment 2010*, Wellington, www.justice.govt.nz/policy/criminal-justice/aml-cft/publications-and-consultation/20110308-NRA-2010-Primary-Document-FINAL.pdf

New Zealand Department of Internal Affairs (2011), *Internal Affairs AML / CFT Sector Risk Assessment,* Wellington, www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf/$file/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf.

New Zealand Securities Commission (2011), *Sector Risk Assessment*, Wellington, www.fma.govt.nz/media/186534/aml-cft-sector-risk-assessment.pdf.

Reserve Bank of New Zealand (2011), *Sector Risk Assessment*, Wellington, www.rbnz.govt.nz/aml/4345201.pdf.

United States:

Money Laundering Threat Assessment Working Group (U.S. Department of the Treasury, *et al.*) (2005), *U.S. Money Laundering Threat Assessment*, U.S. Department of the Treasury, Washington, DC, www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf

Other material

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2004), *Enterprise Risk Management – Integrated Framework*, COSO, website: www.coso.org/erm-integratedframework.htm.

European Network and Information Security Agency (ENISA) (2006), Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment Methods and Tools, Heraklion [Greece], website: www.enisa.europa.eu/activities/risk-management.

EUROPOL (2011), *Organised Crime Threat Assessment*, Europol, The Hague, www.europol.europa.eu/sites/default/files/publications/octa_2011_1.pdf.

The Institute of Risk Management et al. (2002), *A Risk Management Standard*, [United Kingdom], www.theirm.org/publications/PUstandard.html.

International Organisation for Standardisation (ISO) (2009a), *Risk Management – Principles and Guidelines* (ISO 31000:2009), ISO, Geneva, website: www.iso.org.

ISO (2009b), *Risk Management – Risk Assessment Techniques* (ISO 31010:2009), ISO, Geneva, website: www.iso.org.

ISO (2009c), *Risk Management – Vocabulary* (ISO Guide 73:2009), ISO, Geneva, website: www.iso.org.

Organisation for Security and Co-operation in Europe (OSCE) (2012), *OSCE Handbook on Data Collection in Support of Money Laundering and Terrorism Financing National Risk Assessment*, Vienna, www.osce.org/eea/96398.

Standards Australia and Standards New Zealand (2009), *Risk Management – Principles and Guidelines* (AS/NZS ISO 31000:2009), SAI Global, website: www.infostore.saiglobal.com/store.

Treasury Board of Canada (2001), *Integrated Risk Management Framework*, Ottawa, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text.

United Nations Office on Drugs and Crime (UNODC) (2010), *Guidance on the preparation and use of serious and organised crime threat assessments* ["The SOCTA Handbook"], UNODC, Vienna, www.unodc.org/documents/afghanistan/Organized_Crime/SOCTA_Manual_2010.pdf.

U.S. Department of Homeland Security (2010), *DHS Risk Lexicon – 2010 Edition*, Washington DC, www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.