

I. THE INTERNATIONAL MONETARY FUND STAFFS' ML/FT NRA METHODOLOGY

1. **The Fund staffs' methodology for conducting a national money laundering (ML) or financing of terrorism (FT) risk assessment (NRA), follows closely principles established in international standards on risk.** The methodology seeks to help domestic authorities focus on mitigating the risks that flow from substantial ML or FT occurring. It is designed to be applied in varying degrees of detail depending on country preferences. This annex summarizes the main components of the full NRA methodology and describes some processes and tools used.¹ Aspects of the methodology have been applied in more than 50 countries.

2. **ML or FT risk is defined as “the effect of ML- or FT-related uncertainty on a jurisdiction’s government objectives.”** The level of national ML or FT risk is formally defined as the *likelihood* of ML or FT events occurring successfully in a jurisdiction multiplied by the *consequence(s)* of those events. Likelihood is represented as a function (the coexistence) of ML or FT threat and ML or FT vulnerability. The methodology measures net ML/FT risk, that is, the level of risk taking into account the effect of controls on inherent risk. Controls are implemented to reduce inherent risk; thus, they reduce, but their absence or poor effectiveness can never increase, inherent risk. In ML/FT there are two types of controls: general controls and mitigants (e.g., general regulatory requirements); and specific AML/CFT controls, including those implementing the FATF Recommendations.

3. **The NRA methodology relies on a semi-qualitative risk scoring system that focuses on the key risk events associated with the ML or FT process that are thought to make a difference to risk profiles.** Thus, the methodology starts with a pre-determined list of identified generic risks or risk events. The methodology enables the authorities to add additional risk events.

4. **The generic risks identified in the NRA methodology derive from three events that co-exist to enable ML or FT.** First, the launderer holds illegally obtained assets, or terrorist financier holds illegally obtained or legitimate assets that need processing, (a threat); and the perpetrator perceives that there are products, services, assets, or other circumstances that can be abused to meet his or her processing needs (a vulnerability). Second, the launderer or financier perceives that there is little chance of being caught by the authorities during the process (due to vulnerabilities). Third, the launderer perceives that, even if caught, there is little chance of being sanctioned and losing the assets (additional vulnerabilities). Thus, substantial ML or FT is successful if the interrelated risk events identified below occur:

a. **ML or FT is attempted:**

- i. Due to a co-existence of substantial amounts of proceeds of crime (POC), or of terrorist funds that need processing, and

¹ More detailed information is available in Annex 3 of <http://www.imf.org/external/np/pp/eng/2011/051111.pdf>

- ii. Due to the existence of products, services, assets, or other circumstances that the launderer or terrorist financier perceives can be abused to meet their needs; and

b. The perpetrator(s) of the ML or FT is not caught:

- i. if it is attempted, ML or FT will not be detected by the authorities (either directly or indirectly via the efforts of businesses that are required to make suspicious reports); or
- ii. if it is detected, ML or FT will not be investigated adequately by the authorities; or
- iii. if investigated, the perpetrator(s) will not be prosecuted; or
- iv. if prosecuted, the perpetrator(s) will not be convicted, or

c. The perpetrator(s) of the ML or FT is not sanctioned adequately:

- i. if convicted, the perpetrator(s) will not be punished adequately, or
- ii. if punished, the perpetrator(s) will not be deprived of their assets.

5. **Likelihood of these events occurring is derived from related risk analysis modules (RAMs) containing factors, sub-factors and their indicators.** How the generic ML risk events identified above relate to the RAMs is portrayed in Table 1 of this Annex, with the RAMs listed down the right-hand side. Each RAM identifies unique risk factors linked to the relevant threats and vulnerabilities that affect the likelihood of the risk event(s) occurring during any typical twelve-month period, taking into account the effectiveness of existing controls, including AML controls. Each risk factor is informed by a range of relevant indicators, which are analyzed and scored based on pre-determined decision-making criteria. Each indicator is informed by raw data that is scored on a seven-point semi-qualitative ordinal scale according to the pre-determined measurement criteria for each scale. Risk factors are scored as the aggregate of their relevant indicators. The framework's RAMs use both quantitative (data driven and objective) and qualitative (subjective and perceptions-based) indicators drawn from public and private sources. A higher score suggests a higher likelihood that substantial ML or FT abuse will occur successfully.

6. **The NRA methodology produces two proxy indicators of ML/FT consequences—short-term and longer-term—derived largely from the perceptions of officials, using a structured approach to make informed judgments.** The short-term is related to the generic objective of minimizing the amount of ML or FT that occurs successfully during any typical twelve-month period, and is used primarily to help analyze sector risk. More complex indicators of longer-term consequence focus on the potential effect of the likely level of successful ML or FT on various social, economic, and political objectives. The process for both consists of asking the country officials to assess, based on their familiarity with the country's ML/FT environment informed by the NRA process thus far, using pre-determined decision-making criteria and seven-point semi-qualitative ordinal scales, the degree to which country AML/CFT objectives are affected by ML or FT risk events occurring.

7. **The overall level of risk for each event is derived by combining likelihood and longer-term consequences scores, and to assess whether the result falls within acceptable**

bounds. Thus, the analysis is geared toward helping government agencies and policymakers efficiently apply their resources to mitigate the highest risks. The results are presented on a heat map to help identify the relative level of risk between events and their mitigation priority.

8. **An optional sub-component within the methodology produces risk profiles for regulated entities and sectors.** It is geared toward helping regulators and supervisors apply their supervisory resources and also determine areas that might qualify for lower risk exemptions or simplified measures. It thus focuses on the likelihood that particular entity types or sectors will be targeted for ML or FT abuse by launderers and financiers, and uses the short-term consequence analysis described above to derive levels of risk for each entity type and sector. The likelihood analysis derives inherent and net ML and FT likelihood profiles based on sub-factors such as customers, and products and services split into general and trans-national (or cross-border issues) and the adequacy of general and AML/CFT controls.

9. **The fully fledged NRA process comprises seven phases and relies on the authorities' ability to collect and submit statistics and perceptions using web-based data collection tools.** The overall process is iterative, relying on continued feedback from the participating jurisdiction during on-site workshops. The phases and tasks within each phase are:

- a. **Preliminary phase and threat analysis preparation:** The overall objectives of the exercise are agreed, the jurisdiction establishes an NRA coordinating mechanism, fund staff conduct research into the country's POC environment and ML/FT threat indicators, and the authorities complete four surveys (two on data availability and two on domestic and transnational ML and FT threats);
- b. **ML/FT threat:** Fund staff conducts workshops with the authorities to agree final views on domestic and transnational ML and FT threat, including estimates of the magnitude and nature of domestic POC and cross-border flows of POC;
- c. **Vulnerability preparation:** The authorities complete four web-based statistics collection tools (Sectors and Firms Profiles; International Cooperation and Border; Criminal Justice System; and FIU and Reporting) and three perceptions surveys (Sectors and Firms; General Jurisdiction and FIU, Law Enforcement Agency and Criminal Justice System), Fund staff collects publicly available vulnerability information and compile all vulnerability and threat information to generate preliminary likelihood analysis including at the sector level;
- d. **ML/FT vulnerability and likelihood analysis:** Fund staff conducts workshops with the authorities to agree final views on ML and FT vulnerabilities, including a list of main factors that increase and reduce likelihood. The results are combined with those for threat to reach preliminary views on the overall likelihood of the different ML/FT risk events occurring, including within sectors.
- e. **Consequence and overall risk preparation:** The authorities complete two web-based perceptions surveys on ML and FT consequences, Fund staff collects publicly available information related to ML/FT consequence and compile all consequence information to generate preliminary consequence analysis and combine this with likelihood results to produce preliminary risk event heat maps including at the sector and entity level;

- f. **ML/FT consequence and risk analysis:** Fund staff conducts workshops with the authorities to agree final views on ML and FT consequences. Revised heat maps showing levels of risk for each generic risk event and for sectors and entities are presented at separate workshops, discussed, and overall levels of risk and priorities for mitigation are agreed.
- g. **Concluding phase.** Fund staff produces a preliminary draft national risk assessment which is sent to the authorities for review and then finalized for publication.

10. **The NRA methodology produces a range of standardized outputs to help the authorities understand the country's ML/FT risks.** These include a table estimating the domestic proceeds of crime by crime category, summary risk matrix of the main factors increasing and reducing risk, heat maps for risk events and sectors and entities, summary tables relating to sectors and entities, and a national risk assessment document:

- a. A **domestic proceeds of crime summary table** shows for 25 crime categories the estimated range of proceeds generated in each category, a range mid-point, and totals the mid-points to provide an overall estimate of the magnitude of proceeds generated in the country. The mid-points and the total are also expressed as a percentage of the country's GDP. This information may be supplemented by estimates related to the nature and composition of the proceeds in terms of the proportion generated in cash, financial and physical assets and attributable to domestic and trans-national organized criminal groups and other criminals.
- b. A **summary risk matrix** sets out the likelihood scores for each RAM and its associated risk events and the consequences scores for those events. The matrix also sets out a list of the main factors that increase risk scores and those that lower them (i.e., strengths and weaknesses), thus providing the authorities with detailed guidance on which specific factors to address to mitigate the main risks.
- c. **Heat maps** plot the level of risk for all generic risk events and any additional events identified by the authorities by reference to each event's ML/FT likelihood and consequence. Heat maps are also generated to show the level of ML/FT risk for sectors and for entity types within sectors. An example of each type based on actual results is shown in Figure 2 of this Annex.
- d. **Summary tables** for sectors and entities show information such as the number of entities, their total and average assets as well as scores for their inherent ML/FT likelihood, adequacy of AML/CFT controls, and net ML/FT risk. The entities summary can be filtered to generate specific outputs such as, for example, the ten entities with the highest likelihood of being abused for cross-border ML or FT.
- e. The **NRA document** describes in sufficient detail for the intended audience the main risks and their drivers and the process used to arrive at those conclusions.

Figure 1: Summary Diagram of IMF Staff ML Risk Assessment Framework (FT has a separate diagram)

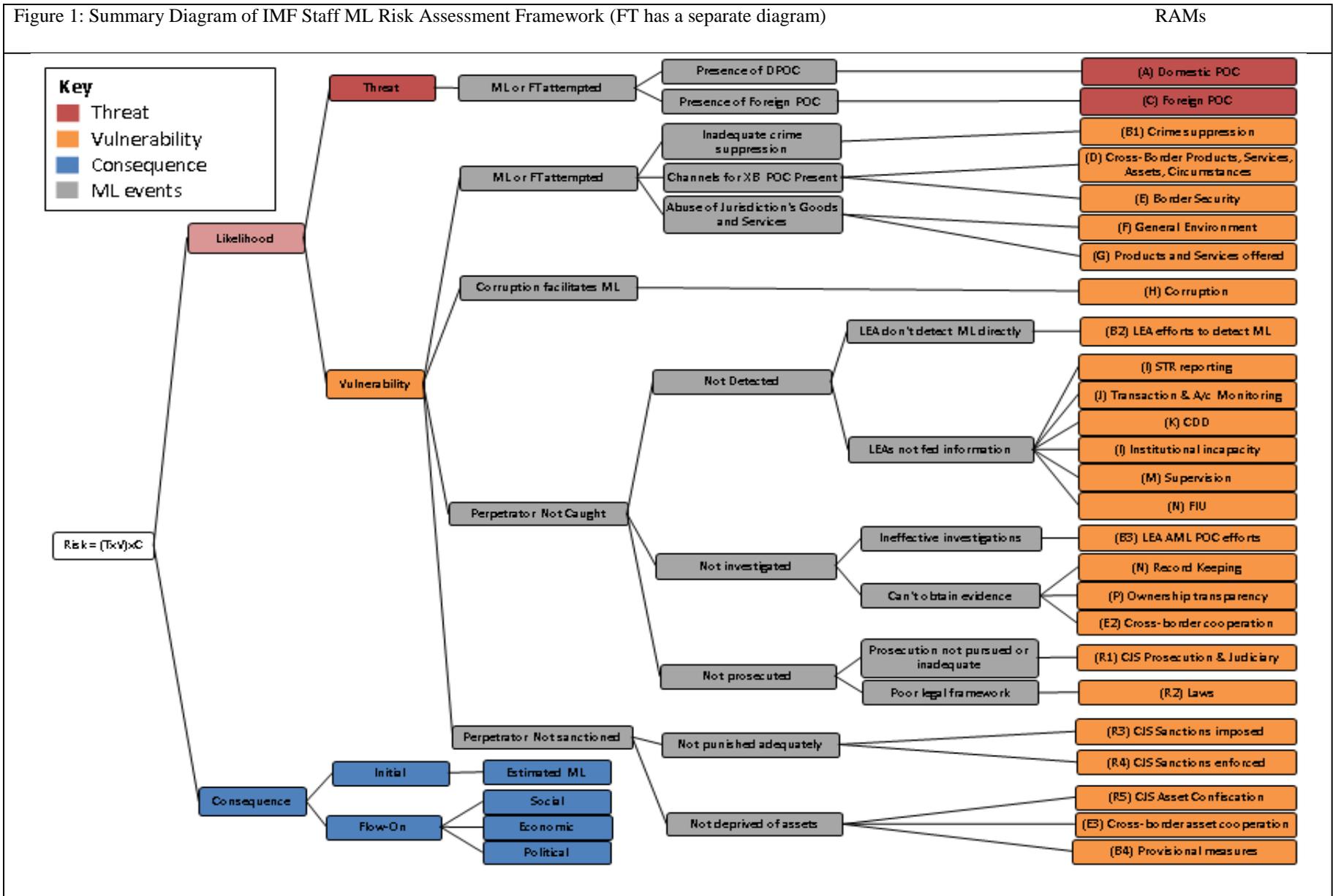


Figure 2: Examples of a ML risk event and sector heat maps

