The World Bank Risk Assessment Methodology

1.   *Background*

World Bank has attached high importance to money laundering and terrorist financing risk assessment from the early years of the recognition of risk based approach in AML/CFT area and has actively helped client countries to assess these risks. In doing so, the World Bank developed two national risk assessment tools (First Generation and Second Generation National Risk Assessment tools) as well as national risk assessment process, with a view to facilitate the risk assessment even in the countries where the data and statistics are limited. The World Bank tools are essentially, although not limited to, self-assessment tools in order to help the countries develop their capacity to collect and analyse the useful data, statistics and information and introduce a risk based approach.

2.   *The NRA Tools Developed by the World Bank*

First Generation Tool

First Generation tool is an Excel-based template that was developed initially by the World Bank and later integrated into the Strategic Implementation Programming (SIP) framework, which is a joint initiative by the World Bank and Asia Pacific Group on Money Laundering (APG). In this regard, refinement of the first generation NRA tool has greatly benefited from participation of APG members and partners.

The first generation NRA tool is offered to client countries by the World Bank also on a stand-alone basis as it may be suitable to them, taking into account their size of economy, sophistication and depth of financial sector and Designated Non-Financial Businesses and Professions (DNFBPs), and complexity of ML/TF crime, among others.

The first generation NRA tool utilises a matrix approach in assessing the ML and TF risks. The risk assessment template focuses on the assessment of threat and vulnerabilities as the main components of the ML/TF risk. SIP NRA Template is an Excel file with 5 assessment areas (ML Prevailing Crime Type/TF Threat Analysis, Legal/Judicial/Institutional Framework, Economic and Geographical Environment, Financial Institutions and DNFBPs), accompanied by summary findings. Each of the assessment areas contains carefully selected indicators to assess threats and vulnerabilities. Two separate risk assessments are undertaken on ML risk and TF risk, using the symmetric risk assessment structure. The worksheets designed for the ML/TF assessment consists of following templates:

Table 1

National ML Risk Assessment Template	National TF Risk Assessment Template
Threat Analysis 1- Prevailing Crime Type **Vulnerability Analysis** 2- Legal/Judicial/Institutional Framework 3- Economic and Geographical Environment 4- Financial Institutions 5- DNFBPs	**Threat Analysis** 1- TF Threat Analysis **Vulnerability Analysis** 2- Legal/Judicial/Institutional Framework 3- Economic and Geographical Environment 4- Financial Institutions 5- DNFBPs

The main difference between ML and TF risk assessment templates is the threat analysis. The objective of ML Threat Analysis is to understand what type of predicate offenses pose a ML threat in jurisdiction based on data and other information collected, and identify origins (both domestic and foreign) and methods of ML. Outcome of such threat analysis would be useful for law enforcement agencies (LEAs) to prioritise their actions. It is also useful for FIU and covered institutions to understand the type of crimes that generate illicit proceeds and different methods of money laundering. On the TF risk assessment side, TF threat analysis also attempts to capture the statistics and any other information but on TF cases and assesses the level and sources of TF threats. Vulnerability analysis section consists of four assessment matrices, each of which focuses on vulnerabilities arising from different areas. "Legal/Judicial/ Institutional Framework" and "Economic and Geographical Environment" assesses the vulnerabilities arising from the factors at the national level, while "Financial Institutions" and "DNFBPs" focuses on vulnerabilities posed by financial institution and DNFBP categories that are present in assessed jurisdiction. The structure of Financial Institutions and DNFBPs matrices are different from the others, and they are designed to enable assessment and comparison of the inherent vulnerabilities as well as net vulnerabilities (after taking into account the control measures) arising from various sectors, institutions or professions. Vulnerability assessment in ML and TF risk assessment templates are very similar and differ in limited number of indicators. This effort was intentionally made in order to allow comparison of ML and TF risk faced by the country.

For each of the indicators in the matrices, a threat, vulnerability or risk level is assessed based on the information and statistics provided. Available information and statistics are filled into designated boxes in the templates. Most of these boxes are designed to capture a short summary of the information/justification. A detailed write up that elaborates the grounds and justification for each assessment, is required in order to ensure the quality and credibility of the assessments.

The template includes pre-identified and carefully selected indicators to assess the ML/TF risks; however, the template can be customised by adding new indicators or amending existing ones, to reflect each country's unique environment.
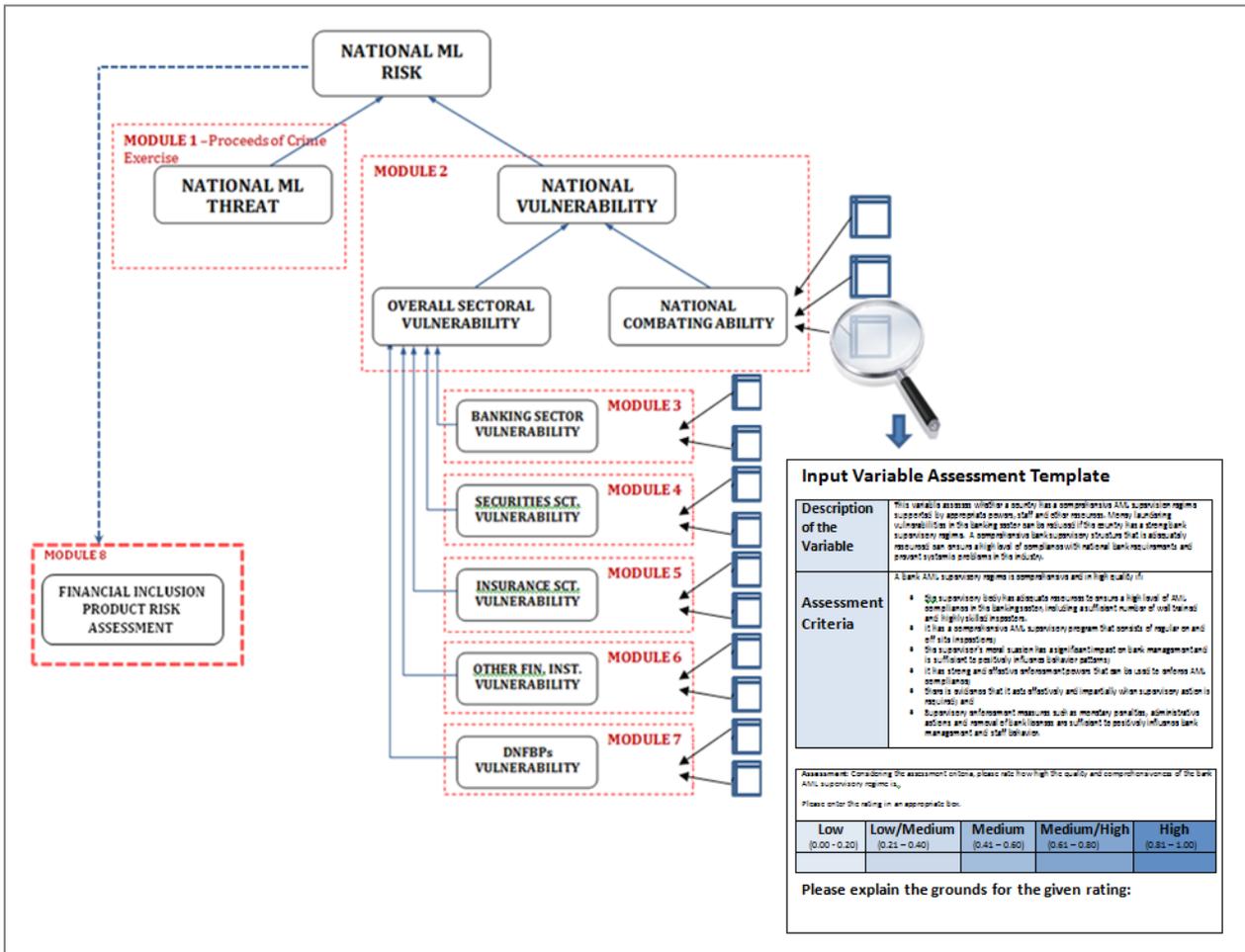
Second Generation Tool

The Second Generation NRA Tool has been developed by the World Bank with a view to enable more rigorous and sophisticated risk assessment. This NRA tool was modeled on the Bayesian Network which utilises the laws of probability at its core of the modeling and analyses the sources and causes of risk. Strong logical sequence of events and causal relations between variables affecting risk is carefully modeled. This enables capturing main drivers of the money laundering risk, formularising the complex environment of money laundering taking into account the interactions among various components of risk and vulnerability and generating a final measure of the risk/vulnerability level. In order to make the tool user friendly and easily accessible, this Second Generation tool has been remodeled based on excel and using weighted averages instead of probabilities, while keeping the logic and concept of ML risk assessment built from the initial Bayesian Network approach.

The Second-Generation NRA tool is a knowledge-based diagnostics and decision making tool that can assist decision-makers to assess and analyse money laundering risk in a jurisdiction. The tool provides a means to understand sources of vulnerability in a country and how various factors that influence the vulnerability are inter-related. The tool can also be used to iteratively observe and analyse the effects of various policy options based on scenarios. For example, the impact of actions (individually or collectively) to reduce the vulnerability can be determined.

The model defines the ML Risk as a combination of national threat and national vulnerability. The national threat module is the "Proceeds of Crime" exercise that provides guidance to countries to assess the ML threat. In assessing national vulnerability, a number of variables are evaluated as main drivers (input variables) of vulnerability to ML. All these input variables constitute the building blocks of a network which ultimately feeds into the national vulnerability node. The general structure of the model is provided in figure 1.

Figure 1

Second Generation NRA Tool consists of 8 modules. Two main modules, namely National Threat Analysis and National Vulnerability Analysis modules that feed into the National ML risk and determine the country's position on the risk map provided in figure 2.

Threat and vulnerability modules are different in their nature. Threat module is not based on modeling but provides guidance to countries to analyse the prevailing predicate offences and proceeds derived from these offences in a particular jurisdiction. A sample template provided to the countries is a starting point to collect data and to trigger the threat analysis to have a better understanding on the scale of the proceeds of crime and associated money laundering. The National Vulnerability Module and the sectoral modules which feed into the former are based on initial Bayesian network modeling. Assessment methodology guides the assessment of "input variables." Inputs variables are identified as the main drivers of the vulnerability. Each assessment template includes the definition of the variable, the criteria that should be used during the assessment and a section designed to record the result of the assessment. Using the criteria, the assessors (of the risk assessment) are asked to assign a score that ranges from 0.0 to 1.0.

For each input variable assessment, assessors are asked to provide a write up to explain the grounds and justification for the assigned rating. This write up is a crucial part of the assessment and needs to include reliable information and analysis, as well as the available data and statistics supporting the assessment.

Scores assigned to each input variable are populated into the Excel model. The excel model combines these scores based on interactions between various factors, weighted averages, and defined prerequisites. The sectoral vulnerability ratings feed into the National Vulnerability Module. In addition to the vulnerabilities arising from the various sectors, National Vulnerability Module requires the assessment of 24 other input variables, which affect the country's ability to combat money laundering.

Second Generation NRA Tool also includes a module on Financial Inclusion Product Risk Assessment. This module aims to assist authorities in evaluating money laundering and terrorist financing risks arising from both existing and emerging/new financial inclusion products and can be used as a basis for designing a risk-based approach in the preventive measures. It can also be used by regulators to design low or lower ML/TF risk financial products. This module is different from other modules and benefits from the output of NRA, rather than feeding into it.

Second Generation NRA tool provides a practical and transparent framework that assist countries to better understand and analyse the complex web of ML risk. Following items can be described as the main strengths of the tool:

- Provides an idea on the overall risk and vulnerability in the country.

- Allows diagnostic and scenario analysis.

- Allows comparison of vulnerabilities arising from various products/services.

- Allows comparison of vulnerabilities arising from various sectors.

- Prioritisation and sequencing of potential AML actions.

- Contributes to the cooperation and collaboration among AML/CFT stakeholders.

3.   *Concept of Risk adopted in the World Bank NRA Tools*

There is no single clear definition of Money Laundering or Terrorist Financing Risk adopted at the international level. However, proposed definitions in this guidance paper focus on three main components, namely threat, vulnerability and consequences.

Concept of risk in the World Bank NRA tools follows a similar approach. The ML risk is considered to be a function of threats and vulnerabilities. The assessment of consequences is included in the assessment of threats and vulnerabilities as opposed to being treated as a separate independent factor. For example, consequences of a ML event in the banking sector are taken into account by determining the different weight each banking sector product has. This weight may be determined by the asset size or volume of transactions of the product.

The result of threat and vulnerability assessment is a risk map which can be used to locate the final risk level of the country as shown in Figure 2 below.

Figure 2

OVERALL MONEY LAUNDERING RISK IN A JURISDICTION
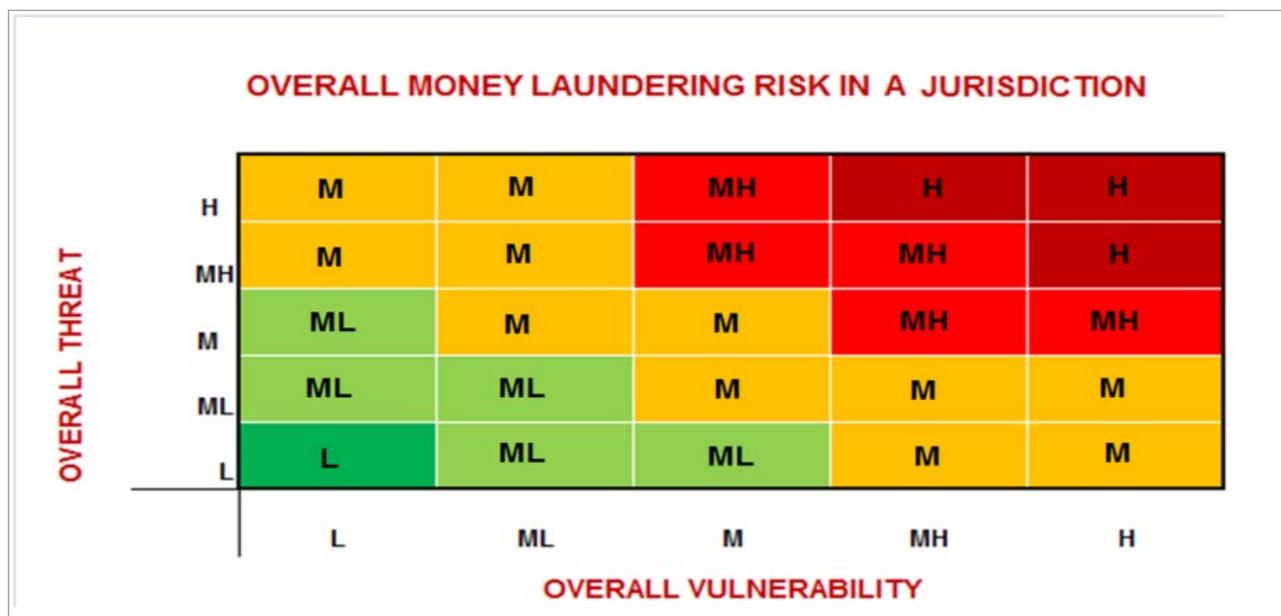
4.   National ML/TF Risk Assessment Process

The World Bank attaches particular importance to the undertaking of risk assessment at the national level, notwithstanding the potential benefit of more focused sector risk assessment. This is because it is extremely important for each country to gain a common understanding among all relevant authorities and stakeholders on the level and nature of ML/TF risk faced by them. Further, the outcome of the NRA should guide sectoral assessments and assessments undertaken by the private sector.

Although it can also be used for assessment by external parties, the World Bank NRA tools are developed and are essentially being offered as self assessment tools. It is an assessment organised, led and owned by the country, while the World Bank provides the risk assessment tools, guidance, and review. One of the main objectives of this self assessment approach is to facilitate the development of the country's own capacity to undertake risk assessments and to implement risk based approach in AML/CFT area. Countries are encouraged to customise and tailor the tools to fit to the specific needs and conditions of the country.

World Bank's NRA Process is designed to facilitate the inclusion of all stake holders in the national risk assessment, which will also enhance the cooperation and coordination among various government agencies as well as the government agencies and private sector, and ensure the completion of national risk assessment in a reasonable time frame.

Establishing a NRA Working Group

In undertaking a national risk assessment, countries are highly encouraged to establish a dedicated NRA working group or a task force. In the Technical Assistance offered by the World Bank, this is a pre-requirement for the project. The NRA Working Group should be composed of all relevant AML/CFT stakeholders. It is usually headed by a lead AML/CFT agency in the country. The Working Group usually

consists of the representatives from, Financial Intelligence Unit, Central Bank, Financial Regulation and Supervision Agency (if exists), Capital Markets Authority, Regulator of the Insurance Market, Tax Authority, Intelligence Agency, Police (Units combating organised crime, drugs, arms trafficking, smuggling etc.), Anti-Corruption Agency, Anti-Drug Agency, Customs Authority, Office of Public Prosecutor, Ministry of Finance, Regulators of other financial services, and authorities related to DNFBPs. Private sector representatives may be invited to the NRA Working Group as a full member or a partial member. For example, the private sector representatives can play a key role in assessing the vulnerabilities of the covered institutions in the preventive measures, but may not be ideally placed if sensitive intelligence is shared.

Given the heavy analytical work involved in the exercise, NRA Working Group member are suggested to be senior technical specialist and expected to stay as the members of the working group throughout the NRA process to ensure the continuity.