WORLD BANK GROUP
Finance & Markets

NRA toolkit

NATIONAL RISK ASSESSMENT TOOL
GUIDANCE MANUAL

MODULE 6
VULNERABILITY OF
OTHER FINANCIAL INSTITUTIONS

JUNE 2015

World Bank Group's National Money Laundering and Terrorist Financing Risk Assessment Toolkit

Disclaimer and Terms of Use

The National Money Laundering/Terrorist Financing Risk Assessment (NRA) Toolkit has been developed by World Bank Group (WBG) staff members to support WBG client countries and jurisdictions in self-assessing their money laundering and terrorist financing risks. The NRA Toolkit contains guidance manuals, including this document; Excel worksheets and the formulas therein; PowerPoint presentations; and any other materials provided as part of the NRA Toolkit. Jurisdictions are advised to use the NRA Toolkit with technical assistance from the WBG to ensure proper application.

The NRA Toolkit is supplied in good faith and is based on certain factors, assumptions, and expert opinions that the WBG may in its absolute discretion have considered appropriate at the time the toolkit was developed. Even if being done through the NRA Toolkit, an NRA is conducted as a self-assessment by a jurisdiction and not by the WBG staff. The user is responsible for any data, statistics, and other information put into the various NRA Toolkit templates, as well as for any interpretation and conclusion based on the results of the NRA Toolkit.

The WBG provides the NRA Toolkit as is and disclaims all warranties, oral or written, express or implied. That disclaimer includes without limitation a warranty of the fitness for a particular purpose or noninfringement or accuracy, completeness, quality, timeliness, reliability, performance, or continued availability of the NRA Toolkit as a self-assessment tool. The WBG does not represent that the NRA Toolkit or any information or results derived from the NRA Toolkit are accurate or complete or applicable to a user's circumstances and accepts no liability in relation thereto. The WBG shall not have any liability for errors, omissions, or interruptions of the NRA Toolkit.

The WBG will not be responsible or liable to users of the NRA Toolkit or to any other party for any information or results derived from using the NRA Toolkit for any business or policy decisions made in connection with such usage. Without limiting the foregoing, in no event shall the WBG be liable for any lost profits—direct, indirect, special, incidental, or consequential—or any exemplary damages arising in connection with use of the NRA Toolkit, even if notified of the possibility thereof. By using the NRA Toolkit, the user acknowledges and agrees that such usage is at the user's sole risk and responsibility.

The NRA Toolkit does not constitute legal or other professional advice, but in particular it does not constitute an interpretation of these Financial Action Task Force (FATF) documents: FATF 40 Recommendations and Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems. The WBG shall not be responsible for any adverse findings, ratings, or criticisms from the FATF or FATF-style regional bodies arising from use of the NRA Toolkit.

Nothing herein shall constitute or be considered a limitation on or a waiver of the privileges and immunities of the International Bank for Reconstruction and Development, which are specifically reserved.

Acknowledgements

The Other Financial Institutions Vulnerability Module of the National ML/TF Risk Assessment Tool has been developed by a World Bank team that was led by Emiko Todoroki and included Kuntay Celik, Louis de Koker, and Ameet Kaur. The module is based on the structure of the Banking Sector Module. The team thanks the staff and the management of the World Bank's Financial Market Stability and Integrity team for their significant contributions, which played key role in the evolution of the module into its current state.

CONTENTS

Important Reminders for the Working Group

- Base your assessments on group discussions to ensure the inclusion of a wide array of perspectives. All members of the Working Group should contribute to discussions, as well as to the overall assessment, as the inclusion of all viewpoints and perspectives will contribute to a higher quality report.
- Keep a record of the key arguments, findings, and conclusions of your discussions. These notes will be important in documenting the analysis and support for the conclusions and findings that will feature in the final report. Assign a note-taker for this task.
- The quality of the output depends on the quality of the input. An unrealistic assessment will reduce the credibility of the overall assessment and will limit the benefits the jurisdiction can derive from the assessment.
- During the assessment, please clearly identify the problems, weaknesses, or gaps by determining what is missing and what is not working. Such an approach will help you draw up your action plans following your assessment.
- Support all your findings and conclusions with clear analysis and documented evidence, in order to demonstrate the basis for each rating.
- Prepare team reports on the key findings and conclusions that are clearly documented with references to underlying sources. These reports will become the building blocks of the overall assessment report.
- For the assessment of Other Financial Institutions, separately assess each of the (relevant) Other FI categories. Save each assessment in a separate Excel file.

1. OBJECTIVES OF THE OTHER FI VULNERABILITY MODULE

This module covers all categories of financial institutions, other than the banking sector, securities sector, and insurance sector institutions, and includes both regulated and unregulated financial institutions.

The main objectives of the module are to:

1. Identify the vulnerability of each of the (relevant) Other FI categories in a country
2. Identify high vulnerability Other FI categories
3. Identify on a needs basis, the products/services/channels[1] offered by these Other FI categories with high ML vulnerability (see Annex 2)
4. Prioritize action plans to strengthen anti-money laundering controls (AML controls) for Other FI categories.

The outcome of the Other FI Vulnerability Assessment is necessary for:

[1] The assessment may include products, services, or channels. For simplicity, this document will subsequently refer only to "products". This reference should be understood as "products, services, or channels".

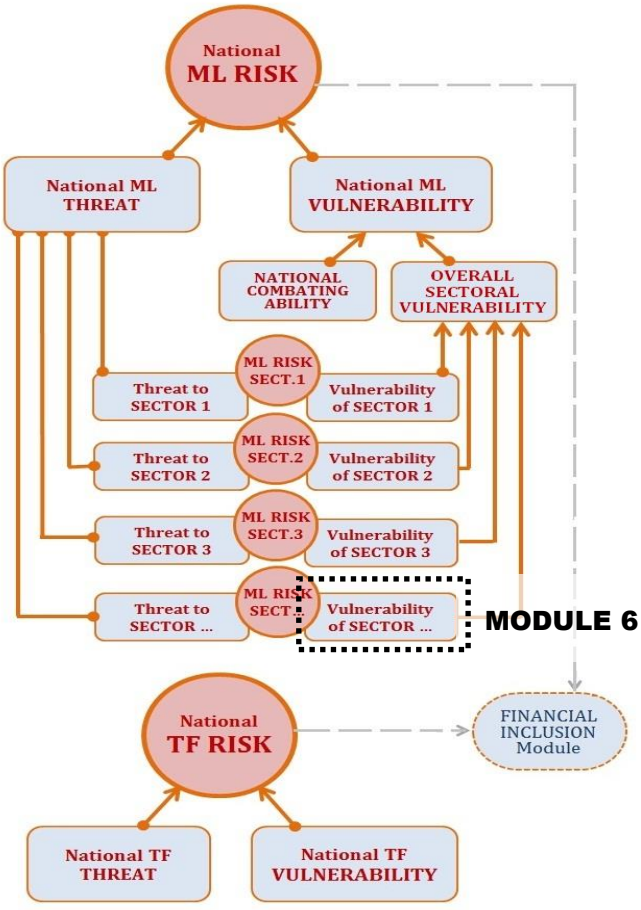
- Designing action plans for more effective AML policies and practices for Other FI categories
- Evaluating the impact of different interventions by regulatory (and other relevant) authorities
- Comparing the level of vulnerability of a particular Other FI category with Other FI categories and the vulnerability level of each of the assessed Other FI categories in relation to other financial sectors
- Ensuring efficient resource allocation
- Developing specific AML controls for highly vulnerable Other FI categories/Other FI products.

2. UNDERSTANDING THE OTHER FI VULNERABILITY MODULE

2.1. Other Financial Institutions' Vulnerability Module in the Big Picture

It is important to understand the module's place and function in the bigger picture of the National Risk Assessment Tool (the tool). As shown in Figure 1, the vulnerability of a certain sector to money laundering and the money laundering threat to that sector together cause the money laundering risk for the sector. In addition to the risk at sector level, the vulnerability of a sector has an impact on the national vulnerability.

Figure 1: Other Financial Institutions Vulnerability Module in the Big Picture of National Risk Assessment Tool



In terms of money laundering (ML), many factors contribute to the overall vulnerability of a country. Some factors have a direct impact, while others are more indirect. The importance and impact of a single factor often depends on the existence, or absence, of other factors. This National Risk Assessment Tool, which has been developed to determine country vulnerability, reflects the various key factors and their relationships.

In this tool, these factors are called "variables." For example, in this module, the variable *Comprehensiveness of AML Legal Framework* indicates the extent to which the laws and regulations of a jurisdiction contribute to the strength of anti-money laundering controls. The ratings assigned to the variables by the Working Group (which carries out the National Risk Assessment) consequently determine the overall vulnerability of the Other FI category.

Note that the module should be run separately for each of the identified Other FI categories within a country. The final vulnerability rating for each of the Other FI category will serve as input to the National Vulnerability module.

Begin this exercise by making a list of the regulated/licensed and unregulated/unlicensed Other FI categories within your country, that have not already been covered in other modules (i.e., the banking sector, securities sector, or insurance sector). This list should include any financial institutions that provide financial services that are not provided by banks, securities firms, or insurance companies.

Below is a suggested list of Other FI categories to provide a starting point for the Working Group. The Working Group (WG) is encouraged to modify the list depending on country context, as well as on the type of institutions present in the country.

Table 1: List of possible Other FI categories:

- Money remitters and transfer agents (including any postal service that offers this service)
- Hire purchase companies
- Mortgage providers
- Pawnshops (if they "lend")
- Providers of deposit boxes
- Cash handling firms
- Card issuers/e-payments (credit/debit/e-cash money)
- Check issuers and cashers
- Foreign exchange dealers (including bureau de change and money changers)
- Undertaking of bill payment businesses
- Credit guarantee corporations
- Mobile financial services providers
- Leasing and factoring institutions
- Other lenders
- Other specialist financial institutions (such as development FIs)

2.2. Assessment of Products on a Needs Basis (Optional Module)

The WG has the option to undertake a more detailed assessment of the products offered by each of the Other FI category. The decision to undertake a detailed product-based assessment for a particular Other FI category should be based on following criteria:

1. Does the Other FI category provide a single type of product, or does it provide various products?
2. If the Other FI category provides various products, does the ML/TF risk differ significantly among the products?
3. Is the Other FI category significant within a country context?

The assessment for products is carried out in the same way as the assessment for categories. Please note that the assessment criteria detailed in Section 4 also applies to the product-based assessment. Up to five different products for each of the Other FI categories may be assessed. For more details on the Product-Based Assessment Module, please refer to Annex 2.

Note that two options of the Excel assessment files are provided. The WG must first choose which Excel assessment file is most appropriate for each of the Other FI categories. The options are: (1) Category Vulnerability Assessment, or (2) Detailed Product-Based Assessment. If the Category Vulnerability Assessment is chosen as the most suitable approach for the particular Other FI category, use *Excel File 6.A Other FI Vulnerability*. If Detailed Product-Based Assessment is chosen as the most suitable approach for the particular Other FI category, use *Excel File 6.B Other FI Vulnerability–Product Based*.

2.3. Variables

In order to build a foundation for subsequent discussion, it is important to first understand the variables on which the module is based. There are two types of variables in the module: (1) input variables, and (2) intermediate variables.

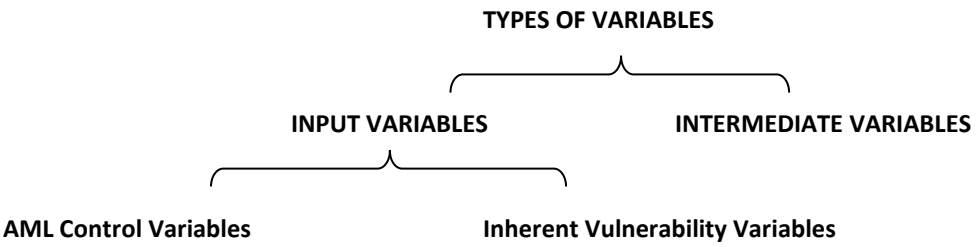
1. **Input variables** require the WG to input an assessment rating. This type of variable breaks down into two subtypes: (1) AML control variables, and (2) inherent vulnerability variables.

    a. *AML control variables.* These factors apply to the entire Other FI category being assessed, and should be assessed at the category level. These input variables relate to the quality and effectiveness of the AML controls, and therefore affect the vulnerability of the entire Other FI category being assessed.

    b. *Inherent vulnerability variables.* These factors relate to specific features and users of the businesses/institutions that make up the Other FI category. An example is the client base profile. As the client base profile for each Other FI category may vary, and consequently affect its vulnerability, it is necessary to assess the risks related to the client profile separately for each of the Other FI categories.

2. **Intermediate variables** are broad and high-level factors that cannot be assessed directly. They therefore need to be disaggregated into their constituent parts in order to be assessed. The module determines intermediate variables automatically, based on the ratings entered for the input variable. Though assessment is undertaken at the input variable level, intermediate variables are very important in the network structure. The next section explains the roles of the input variable and intermediate variables in more detail. Descriptions of the types of intermediate variables can be found in Section 5.

Figure 2: Variables in the Other FI Vulnerability Module
Default: Category Vulnerability (Non-product-based assessment)



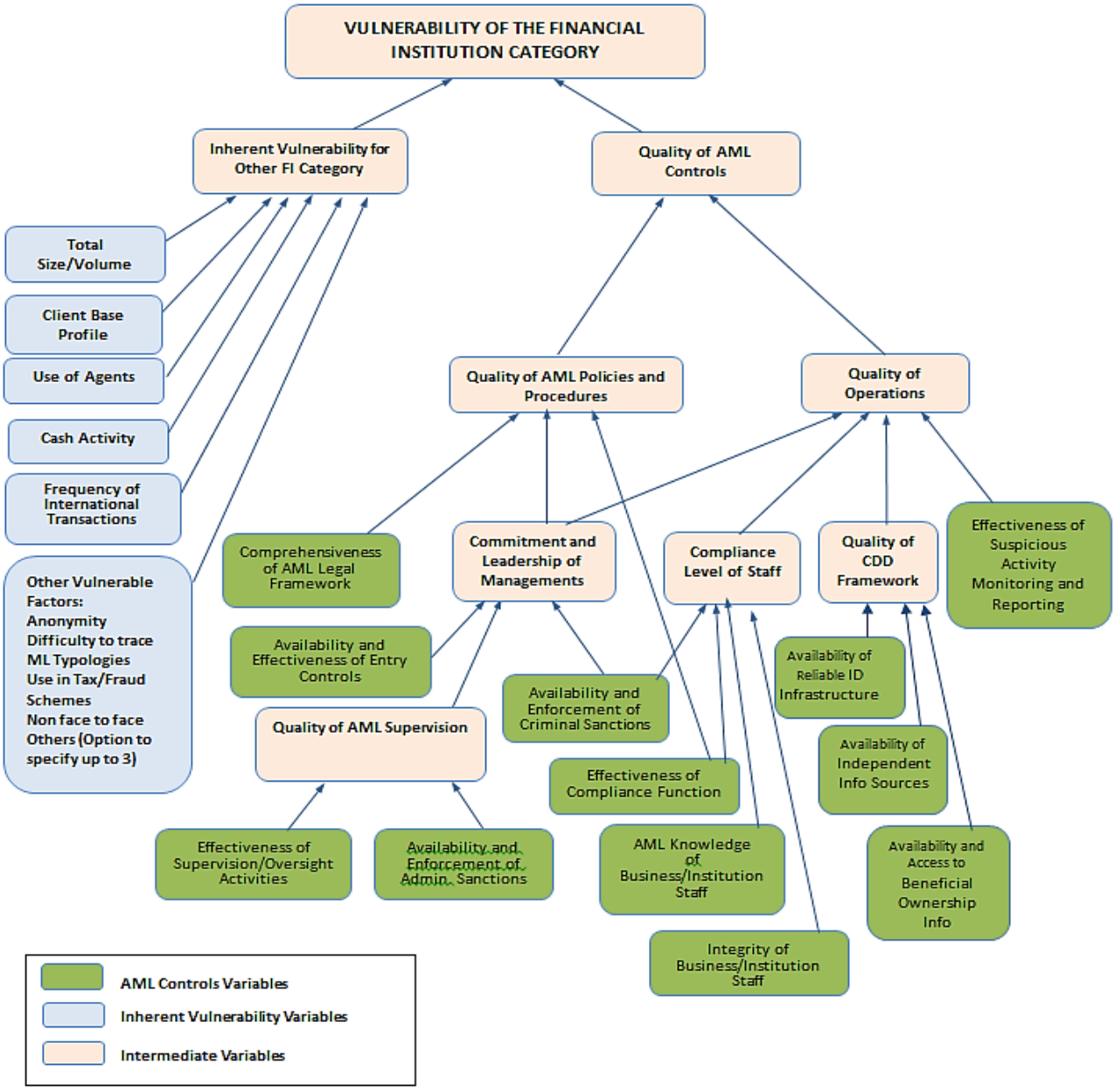
The relationship between this breakdown and the module structure in Figure 3.a is as follows:

- Intermediate variables (pink boxes) do not require assessment.
- AML control variables (green boxes) need to be assessed for the entire Other FI category.
- Inherent vulnerability variables (blue boxes) need to be assessed for each of the Other FI categories.

2.4. Module Structure (The Network)

As illustrated in Figure 3.a, the final vulnerability rating of the Other FI category being assessed is determined by a range of inherent vulnerability factors related to the assessed Other FI category and a range of AML control factors applied to the assessed Other FI category.

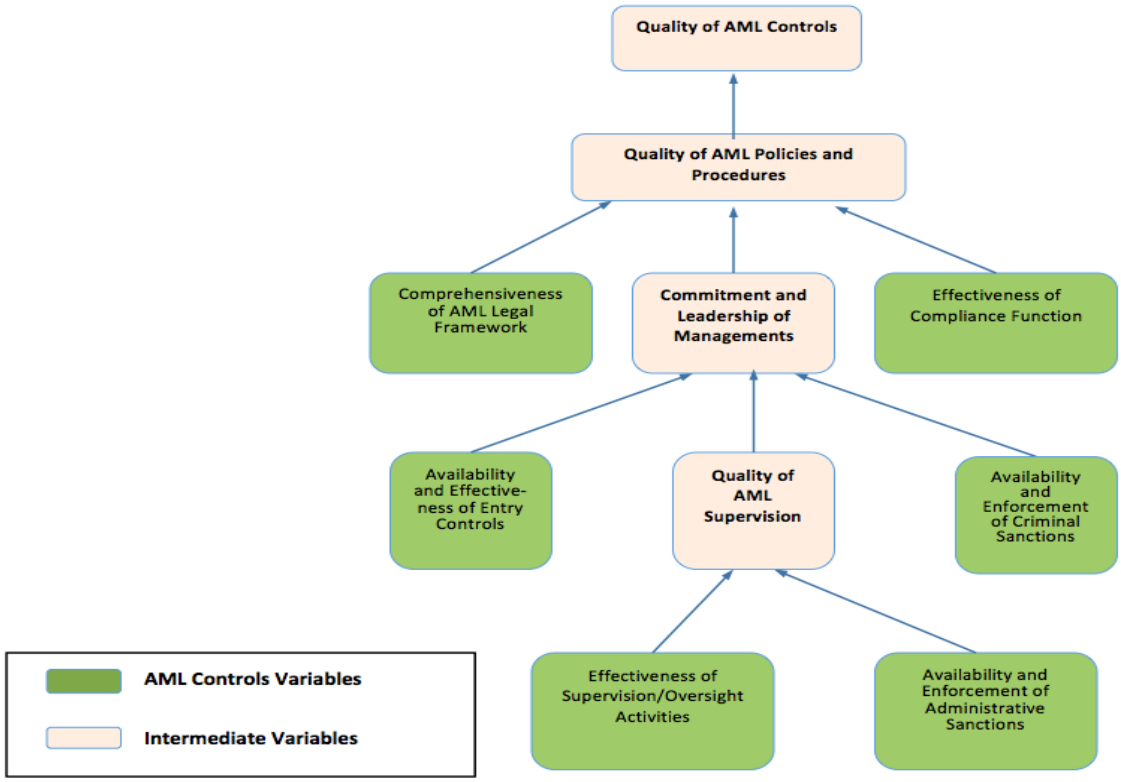
Figure 3.a: Other FI Category Vulnerability Module Structure (Excel File 6.A)



2.5. The Logic Behind The Network

In Figure 3.b, a small part of the structure is highlighted, in order to clarify the logic of the module. In particular, this refers to how the **input variables** and **intermediate variables** contribute to determining overall vulnerability. Please refer to Figure 3.a to see how Figure 3.b fits in to the whole structure.

Figure 3.b: Part of the Network Structure



In order to demonstrate how input variables work, this example will focus on the variable *Availability and Enforcement of Administrative Sanctions*. Consider how the availability and enforcement of administrative sanctions in the Other FI category being assessed affect the quality of AML controls. Clearly there is an impact, but not a direct impact.

The *Availability and Enforcement of Administrative Sanctions* increases the supervisory authority's ability to apply pressure on the managements of the assessed businesses/institutions that make up a particular Other FI category. This supervisory pressure strengthens the commitment of the assessed businesses/institutions managements to ensure AML compliance and to show leadership in the matter. As a result, the managements start to take action to improve the quality of their internal AML policies and procedures, as well as its implementation. As a result, the Other FI category develops better AML controls, and consequently the vulnerability of the particular Other FI category decreases.

However, the input variable *Availability and Enforcement of Administrative Sanctions* is not the only factor that determines the quality of AML supervision. Other factors also need to be taken into account, such as the power, capacity, and effectiveness of the supervisory agency. These other factors are captured in a second input variable, *Effectiveness of Supervision/Oversight Activities*. Assessing this second variable together with *Availability and Enforcement of Administrative Sanctions* will provide a more accurate assessment of the *Quality of AML Supervision*. Note that the *Availability and Enforcement of Administrative Sanctions* and *Effectiveness of Supervision/Oversight Activities* are both input variables to the *Quality of AML Supervision*, which is itself an intermediate variable. Input variables require direct inputs from the WG, while the intermediate variables do not – as illustrated in Figure 3.a (i.e., intermediate variables have arrows feeding into them, while input variables do not). For descriptions of intermediate variables, refer to Section 5.

Factors that determine the vulnerability of Other FI category

There are four factors that determine the vulnerability of Other FI category.

1. The network structure of the module
2. The relative weight of the input variables and intermediate variables
3. The defined conditions (prerequisites) for intermediate variables
4. The assessment ratings of the input variables as assigned by the WG.

The assessment ratings of input variables are assigned by the National Risk Assessment Working Groups of the country. The other three factors mentioned in the above list are based on the underlying assumptions and structural components of the module, as developed by the World Bank. These modules contain default (pre-requisite) formulas determined by the World Bank. These provide assessment results for intermediate variables based on weighted linking of the underlying relationships of input variables. These formulas can be viewed (i.e., "unhidden") – see Annex 1 for further information. Changes to these formulas can only be made by the World Bank. If changes are required, contact the World Bank NRA Team for further information.

The calculation

The formulas that have been built into the module make it possible to combine the assessment results of input variables and calculate the ratings for intermediate variables. Each variable in the module has been assigned a weight, and the underlying relationships between the variables of various levels have been determined by setting up certain pre-conditions. To make the use of the tool relatively easy, the default settings of the module hide the tab that gives details of the weights and pre-conditions. However, the user can make them visible again with a simple Excel procedure. (For more details, see the Excel instructions in the Annex. More on the logic and design of the tool can be found in the PowerPoint presentation "The Logic behind the Tool", which is included in the NRA training package.)

3. GENERAL GUIDANCE FOR THE ASSESSMENT

3.1. Introduction

The assessments need to be made using the assessment worksheets (see Section 4). Each assessment worksheet describes one input variable and the criteria to be considered in assigning ratings. For example, to determine the assessment rating for the input variable *Comprehensiveness of AML Legal Framework*, the WG would assess the degree of comprehensiveness of AML laws and regulations. If all the criteria are met fully and perfectly, the input variable can be rated as Excellent (1.0). The WG should use its professional judgment and expertise to determine what ratings to assign when one or more assessment criteria are not satisfied.

The ratings of the input variables affect the vulnerability of the Other FI categories in various directions.

- **AML controls.** Higher ratings reduce the vulnerability of the Other FI categories; lower ratings increase the vulnerability of the Other FI categories.
- **Inherent vulnerability variables.** Higher ratings increase the vulnerability of the Other FI categories. Conversely, lower ratings decrease the vulnerability of the Other FI categories.

Each assessment worksheet includes the definition of the assessed variable, a list of assessment criteria, and guidance on how to support the assessment. The WG should avoid simply averaging the ratings if some of the assessment criteria are met while others are not. This is because an important deficiency in one of the assessment criteria may offset the positive ratings, or impact, of other items. Ratings should therefore be decided on the basis of professional judgment, experience, and group discussion, with all viewpoints being taken into account.

The most important thing to keep in mind is that the resulting National AML/CFT Risk Assessment Report will be one of the most important, foundational, and closely scrutinized documents during an AML/CFT evaluation. The AML/CFT Evaluation team will view the evidence, analysis, and justification that supports ratings as being far more important than the ratings themselves. Any input variable rating will therefore be meaningful only to the extent that it is supported with adequate and credible analysis and evidence. The worksheets in Section 4 have been provided to enable the WG to document the reasons and basis for ratings, including the supporting data and information on each of the input variables. The group work during the assessment generates valuable discussions and perspectives. A note-taker in each group should record these in the working papers. Such records are important because they highlight the specific problems that will inform the design of the action plan in the next steps. These working papers will also be used to compile the National ML/TF Risk Assessment Report when the assessment is repeated at some point in the future.

3.2. Organization of the Assessment Work

The assessment consists of two main stages:

Stage 1. Assessing and rating the input variables, and supporting the assessment with data and information.

Stage 2. Filling in the Excel file, and obtaining and interpreting the outputs.

Stage 1 is the most important and time-consuming, and therefore calls for good time management. During the first workshop, preliminary ratings can be inserted in the Excel file. In this way, the WG can obtain a good understanding of how the Excel tool works. The preliminary ratings can, and should, be amended as the WG conducts additional fact -finding.

Section 4 and 5 is related to Stage 1, while Annex 1 provides detailed instructions on how to use the Excel file (Stage 2). During the WG sessions in the first workshop, allocate most of your time to Stage 1, and save the final two hours for Stage 2.

Common input variables that appear in all modules

The input variables *Availability and Access to Beneficial Ownership Information*, *Availability of a Reliable Identification Infrastructure*, and *Availability of Independent Information Sources* are included in every module of the tool, and are assessed at a national level. The assessment rating for these variables should be consistent across all modules. Unless there is clear rationale behind assessing these variables separately, the Other FI WG can use the ratings assigned to these variables by the National Vulnerability or Banking Sector WGs.

3.3. Period for Information and Data Collection

The World Bank's National Risk Assessment methodology is based on informed expert judgment. The purpose of the data and information collection is to inform and facilitate sound judgment. The most appropriate period over which data and information should be collected depends on what can better support the judgment as of the assessment date. For some indicators, data from the past twelve months can provide the most meaningful insight. In other cases, however, it may be necessary to collect information/data from the previous five years, as only then may it be possible to discern relevant trends and cumulative amounts.

Table 2: Guidance on information and data collection period

INDICATORS	**Information and data collection period**
Quantitative indicators of vulnerabilities	Ten, five, or three years, depending on the availability of the data.
Qualitative indicators of vulnerabilities	Do not require a strict timeframe. The most meaningful information is the most recent information. Obtain as much information from the last five years as possible.

Since this is not a statistical model, it is not strictly necessary that the data collection period be the same for all indicators. Using different data collection periods in different sections will not be problematic. The indicators for each jurisdiction are to be analyzed, and judgments should be made regarding the current situation.

3.4. Possible Sources of Information and Data

The following list provides guidance on which data and information sources can be used for completing the assessment.

- Statistics (national and international)
- Intelligence
- Interviews with relevant authorities/interest groups/market participants
- Focus group meetings with relevant authorities/interest groups/market participants
- Surveys of general public/focus groups
- Reports by international organizations (e.g., United Nations, World Bank Group, International Monetary Fund, World Customs Organization, and World Trade Organization)
- Reports by international standard-setting bodies (e.g., Financial Action Task Force and FATF Style Regional Bodies)
- Reports by governments/think-tanks/civil society organizations/private institutions
- Books/articles/reports based on academic research
- Media/Internet/other sources of public information.

The above general sources are applicable to all of the input variables to be assessed. In addition to these general sources, the worksheet for each indicator contains specific guidance on the information and data collection for that specific indicator.

4. ASSESSMENT WORKSHEETS FOR INPUT VARIABLES

4.1. Assessment Worksheets for General Input Variables

This section includes guidance on how to assess AML Control variables. Each assessment worksheet contains a description of the variable, the assessment criteria, brief guidance on how to support the assessment, and an assessment section in which to record the rating.

The AML control variables for this module relate to the strength of the AML controls. This assessment is category-wide, and therefore should consider all the businesses/institutions within the Other FI category being assessed. Note that this assessment needs to be undertaken separately for each of the Other FI category assessed. The AML control variables are as follows:

1. *Comprehensiveness of AML Legal Framework*
2. *Effectiveness of Supervision/Oversight Activities*
3. *Availability and Enforcement of Administrative Sanctions*
4. *Availability and Enforcement of Criminal Sanctions*

5. *Availability and Effectiveness of Entry Controls*
6. *Integrity of Business/Institution Staff*
7. *AML Knowledge of Business/Institution Staff*
8. *Effectiveness of Compliance Functions (Organization)*
9. *Effectiveness of Suspicious Activity Monitoring and Reporting*
10. *Availability and Access to Beneficial Ownership Information*
11. *Availability of a Reliable Identification Infrastructure*
12. *Availability of Independent Information Sources.*

In order to better understand how these variables impact the vulnerability of the Other FI categories being assessed, refer to Figure 3.a.

At this stage, the assessment does not focus on vulnerability directly. Rather, the assessment is more about the quality, effectiveness, or level of these variables. Based on these input variables, the vulnerability of the Other FI category being assessed is determined by the module. For example, the assessment should rate how effective the supervisory body is, not how its effectiveness impacts the vulnerability of the Other FI category being assessed. This basic principle applies to all input variables.

The input variables are designed to capture the main drivers of vulnerability in a jurisdiction, and do not necessarily overlap with FATF Recommendations. Still, this self-assessment can be partially supported by the findings from the mutual evaluation report (if relevant). However, this does not mean that the mutual evaluation report (MER) findings are binding on the WG. The WG is encouraged to make use of many different reports and analyses that assess the ML risk of a country.

Recording the grounds of the assessment

The assessment worksheets for the module are in the following pages of this section. In addition to assigning a rating to each of the input variables, the WG should record the justification for these ratings by using a copy of the table in next page. The table should be extended as necessary.

Completing the Entry Page tab in Excel file

The results of the AML controls assessments should be filled in on the **Entry Page** tab of the Other FI Category Vulnerability Excel file. This should be done only after the assessments of all the variables are completed. Refer to Annex 1 for detailed instructions on how to use the Excel file.

Name of input the variable:
Assigned rating and brief reasoning behind it:
Discussion of assessment criteria, and the data and information that supports the assessment:
Deficiencies/problems/room for improvement:

4.1.1. Comprehensiveness of AML Legal Framework

Variable description

This variable assesses whether a country has comprehensive AML laws and regulations regarding AML preventive measures and AML supervision for the Other FI category being assessed.

This input variable **does not** assess the implementation of AML laws and regulations (which is assessed by other input variables). Rather, it is related to the AML legal and regulatory framework for the Other FI category being assessed.

Assessment criteria

A country has comprehensive AML laws and regulations regarding preventive measures and supervision in place for the Other FI category being assessed if they conform to international standards on:

- Customer Due Diligence (risk-based, including verification of beneficial ownership of customers that are natural persons/legal entities/legal arrangements)
- Record-keeping
- Enhanced Due Diligence for Politically Exposed Persons (PEPs) and high-risk countries
- Reliance on Customer Due Diligence by third parties (including introduced business)
- Suspicious Transaction Reporting (STR)
- Registration or licensing
- Tipping-off and confidentiality
- Internal controls, foreign branches, and subsidiaries
- Regulation and supervision/oversight of Financial Institutions (FIs).

Possible sources of information and data

- Relevant laws, regulations, and enforceable guidance (related to assessment criteria above)
- Interviews/consultations with regulatory/supervisory authorities (e.g., a Self-Regulatory Body [SRB]), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of managements and staff from businesses/institutions that make up the Other FI category.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0 ☐	0.9 ☐	0.8 ☐	0.7 ☐	0.6 ☐	0.5 ☐	0.4 ☐	0.3 ☐	0.2 ☐	0.1 ☐	0.0 ☐

4.1.2. Effectiveness of Supervision/Oversight Activities

Variable description

This variable assesses the effectiveness of AML supervision/oversight activities for the assessed Other FI category. An effective supervisory regime is one that has a comprehensive legal and regulatory framework, which is supported by appropriate powers and is well resourced, and employs a risk-based approach to on-site/off-site monitoring and inspections.

This variable **does not** assess the availability and enforcement of sanctions. Sanctions are assessed below as two separate variables in relation to administrative and criminal sanctions.

Assessment criteria

The AML supervision/oversight activities are effective when the supervisory body (which can be a SRB):

- Is clearly identified within the laws and regulations of a country
- Has appropriate authority and mandate to conduct AML compliance supervision
- Carries out its supervisory activities within a comprehensive supervisory framework (which includes clear supervision policies, procedures, and manuals)
- Possesses a good understanding and appreciation for the ML risks within the Other FI category being assessed
- Has a sufficient number of trained staff
- Equips staff with the necessary skills and up-to-date knowledge (including the nature of the businesses/institutions, clients, and the products offered by the Other FI category being assessed) to carry out AML supervision
- Has the necessary resources to ensure AML compliance (technical capacity, budget, tools, etc.)
- Carries out a comprehensive, risk-based supervisory program that consists of on-site and off-site monitoring and on-site inspections on both regularly scheduled cycles and periodic spot-checks (risk-based and as necessary)
- Reports and records the examination results in a systematic way and is able to effectively use these records for policy purposes
- Exercises moral suasion that has a significant impact on the management of the businesses/ institutions (of the Other FI category being assessed), and is sufficient to positively influence behavior patterns
- Can demonstrate that supervisory powers are exercised effectively and impartially.

Possible sources of information and data

- Relevant laws and regulations, policies, procedures, and manuals (including how the risk-based approach is determined)
- Statistics on the number of supervisory staff, and information on their level of training, knowledge, and skill-set
- Information on the type(s) and methods of supervision/monitoring activities and findings
- Statistics on the number of businesses being monitored or inspected (on-site/off-site), and information as to the scope, frequency, and intensity of the supervision/oversight activities
- Statistics and information on the main findings of the monitoring and the on-site/off-site inspections
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff of businesses/institutions that make up the Other FI category.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1	0.0

4.1.3. Availability and Enforcement of Administrative Sanctions

Variable description

This variable assesses whether the country has a wide range of effective, proportionate, and dissuasive administrative sanctions to deal with natural/legal persons in cases of noncompliance with AML laws and regulations. Sanctions should be applicable to businesses/institutions as well as individual directors, management, and staff. The more the sanctions are effective, proportionate, and dissuasive, the more likely it is that management and staff members will comply with AML laws and obligations.

This variable also assesses whether country takes administrative enforcement action against businesses/institutions, or individual members of management or staff, in cases of noncompliance with AML obligations. Consider the number of administrative actions that have been taken against businesses/institutions and their staff over the past few years for noncompliance with AML obligations.

Assessment criteria

If the following criteria are met, it indicates that effective, proportionate, and dissuasive administrative sanctions are in place:

- There is a wide range of administrative sanctions in force for noncompliance with AML obligations (such as monetary penalties, administrative actions, removal of critical staff, and suspension/revocation of business licenses).
- Administrative sanctions are sufficient to positively influence management and staff behavior at businesses within the Other FI category being assessed.

If the following criteria are met, it indicates that a country enforces its AML obligations in cases of noncompliance:

- There is a record of administrative enforcement actions that have been taken in the past by law enforcement authorities for noncompliance with AML requirements within the Other FI category being assessed.
- Most persons working within the Other FI category being assessed believe that administrative enforcement action would be initiated in cases of noncompliance with AML requirements.

* The adequacy of the administrative sanctions may need to be assessed in context with the criminal sanctions. The balance and preference between the administrative and criminal sanctions may differ among countries.

Possible sources of information and data

- Specific legal and regulatory provisions on administrative sanctions
- Statistics on number (by type) of past administrative enforcement actions by relevant authorities
- Information as to steps taken (or not taken) by the Other FI category being assessed to remedy infractions
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed, including SRBs and professional associations (including forms of enforced sanctions, such as disciplinary hearings or revocation of membership)
- Surveys of management and staff from businesses/institutions that make up the Other FI category.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0 ☐	0.9 ☐	0.8 ☐	0.7 ☐	0.6 ☐	0.5 ☐	0.4 ☐	0.3 ☐	0.2 ☐	0.1 ☐	0.0 ☐

4.1.4. Availability and Enforcement of Criminal Sanctions

Variable description

This variable assesses whether the country has a range of effective, proportionate, and dissuasive criminal sanctions, which are applicable to natural/legal persons in cases of noncompliance with AML laws and regulations. This should include sanctions for serious and deliberate (or criminally negligent) breaches that may be ancillary to money laundering offenses. Sanctions should be applicable to the businesses/institutions within the Other FI category being assessed, as well as to individual managers and staff in relation to the conduct of their activities within or from the country.

This variable assesses not only legal frameworks, but also the actual enforcement of criminal sanctions against businesses/institutions and individual members of management or staff (of the Other FI category being assessed) in cases of noncompliance with AML obligations.

Assessment criteria

The following criteria indicate that effective, proportionate, and dissuasive criminal sanctions are available and effective:

- There are appropriate criminal sanctions in place for noncompliance with AML obligations.
- Most persons within the Other FI category being assessed regard the criminal sanctions regime as sufficiently dissuasive to positively influence individual behavior patterns.
- Criminal sanctions are also applicable for appropriate ancillary offenses to the offense of money laundering.

The following criteria indicate that a country enforces its AML obligations in cases of noncompliance:

- Most persons working within the Other FI category believe that criminal enforcement actions would be initiated in cases of breaches of AML-related obligations.
- Criminal enforcement against businesses/institutions and their staff from the Other FI category being assessed — with regard to other financial crimes (such as fraud)—may also serve to give an insight into the perception of enforcement within the Other FI category being assessed.
- There is a record of convictions, and criminal enforcement actions that have been taken in the past by law enforcement authorities regarding breaches of AML obligations within the Other FI category being assessed. Consider the number of investigations, prosecutions, and convictions, as well as other available evidence on enforcement.

Possible sources of information and data

- Relevant laws (specific provisions on criminal sanctions and enforcement), including relevant ancillary offenses to ML
- Statistics on past and ongoing criminal investigations, prosecutions, and convictions by domestic law enforcement (and other relevant authorities), with respect to the Other FI category being assessed
- Statistics on criminal enforcement actions carried out by foreign law enforcement (and other relevant authorities) against the businesses/ institutions and individual members of staff from the Other FI category being assessed, and whether (as well as what form and extent) the country provided informal/formal assistance to the investigation and prosecution
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of managements and staff from the businesses/institutions that make up the Other FI category.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1	0.0

4.1.5. Availability and Effectiveness of Entry Controls

Variable description

This variable assesses the availability and effectiveness of entry controls (including licensing, registration, or other forms of authorization to operate) required for the Other FI category. A country has effective entry controls if there is a comprehensive legal and regulatory framework, which provides authorities with appropriate powers, a sufficient level of staff, and other resources with which to carry out their duties. Effective entry controls help to reduce money -laundering vulnerability, and ensure a higher level of compliance with AML requirements.

Assessment criteria

Entry controls are effective when the licensing body:

- Is clearly identified in the laws and regulations,
- Possesses a good understanding and appreciation for the ML risk within the Other FI category being assessed
- Effectively carries out its licensing and entry control duties
- Has a clear and comprehensive framework for the licensing and registration requirements of the Other FI category being assessed, including:
  - A "fit and proper" test designed to prevent criminals (or their associates) from being granted a business license, being the beneficial owner of a significant controlling interest within a business, or holding a significant management position within a business
  - Appropriate educational and professional certification requirements for key directors and senior management
  - Requirements for all licensees to have adequate AML compliance controls in place, including compliance manuals and the appointment of well-qualified internal controls/compliance staff
  - Possesses adequate resources to ensure the quality implementation of entry controls for the Other FI category being assessed, including a sufficient number of well-trained and highly skilled personnel to screen, vet, and approve all applications and supporting documentation.

Possible information and data sources

- Licensing and registration laws and regulations, policies, procedures (including application forms and supporting documentation), and manuals for supervisory staff
- Statistics on the number of staff screening and vetting licensing applications
- Statistics on the license applications received and the licenses actually granted
- Statistics and information on the licenses not granted, or later suspended/revoked for failure to meet AML controls
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff from the businesses/institutions that make up the Other FI category.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0 ☐	0.9 ☐	0.8 ☐	0.7 ☐	0.6 ☐	0.5 ☐	0.4 ☐	0.3 ☐	0.2 ☐	0.1 ☐	0.0 ☐

4.1.6. Integrity of Business/Institution Staff

Variable description

This variable assesses whether the directors, managers, and staff of businesses/institutions act with integrity. This means that staff does not act in a willfully blind manner, collude with criminals, or act corruptly. In addition, they should take care that they do not become unwittingly involved, as "innocent agents" of criminals seeking to use their products or specialized knowledge/skills.

If staff members collude with criminals, or undermine AML controls by acting corruptly, firms are vulnerable to money laundering abuse. Consider (1) the effectiveness of staff vetting programs within the Other FI category being assessed, (2) the incidence of disciplinary action for breach of integrity related rules, and (3) the number of criminal cases against staff members.

Assessment criteria

Staff in businesses/institutions (of the Other FI category being assessed) are regarded as acting with integrity if the following criteria are met:

- Businesses/institutions generally regard their staff members as secure from corruption by criminals.
- The incidence of integrity failure (e.g., negligent or "willful blindness" to suspicious transactions) involving staff is low (but consider whether there is underreporting of incidences of integrity failure).
- There are appropriate mechanisms in place to protect managers and staff against any negative consequences that result from reporting suspicious transactions, or other actions that comply with AML obligations.

Possible sources of information and data

- Relevant laws/regulations (including specific provisions on confidentiality mechanisms in place for staff when reporting suspicious, or other relevant transactions)
- Information on staff vetting and training programs (of the Other FI category being assessed)
- Statistics on integrity breaches by managers and staff within businesses/institutions (of the Other FI category being assessed) and information as to the resulting disciplinary actions taken
- Statistics on the number of criminal cases (including money laundering cases) against businesses and individuals of the Other FI category being assessed
- Findings of the AML on-site inspections and off-site monitoring for the Other FI category being assessed
- Statistics on the number (and type) of administrative enforcement actions taken against staff from the businesses/institutions (of the Other FI category being assessed)
- Review of reports/records of the internal control/compliance units in businesses/institutions (of the Other FI category being assessed)
- Historical data regarding incidents, or breaches, by staff from the Other FI category being assessed (kept by businesses for operational risk management purposes)
- General level of integrity, or the operating environment within the country (refer, for instance, to Transparency International's Corruption Perception Index)
- Reputation of the Other FI category being assessed, concerning their involvement in financial crimes (including tax evasion)
- Interviews/consultations with regulatory/supervisory authorities (e.g., a SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed, including SRBs (particularly internal control, or compliance, units) and professional associations
- Surveys of management and staff from businesses/institutions that make up the Other FI category.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1	0.0

4.1.7. AML Knowledge of Business/Institution Staff

Variable description

This variable assesses how well staff from businesses/institutions within the Other FI category know and understand their AML obligations.

Assessment criteria

Staff from businesses/institutions in the Other FI category being assessed have the required AML knowledge if the following criteria are met:

- Appropriate AML training programs and materials are available for staff. Consider the frequency, level, and types of training available for different types of staff, as well as the quality of the training.
- Training programs are designed to ensure that all appropriate staff members are trained.
- All staff members are required to undergo ongoing training to ensure that their knowledge of AML laws, policies, and procedures is appropriate and up-to-date. Keep in mind that if the businesses conduct business with clients in other jurisdictions, their knowledge should also extend to the AML laws and regulations of those jurisdictions.
- Staff members have a good knowledge of and are regularly updated on domestic and transnational money laundering schemes and typologies, including actual and potential misuse of the businesses and specialized knowledge and skills of their professionals and their products and services.
- Staff members are aware of AML compliance and reporting procedures and obligations.
- Staff members understand the legal consequences of AML compliance breaches.

Possible sources of information and data

- Relevant legal and regulatory framework pertaining to staff knowledge (including as part of entry controls/renewal of business licenses or certifications)
- Statistics and information on the overall quality of AML training activities held by the businesses/institutions of the Other FI category being assessed, and whether such training is mandatory or voluntary
- Data on frequency of training, hours of training, number of trainees, and level and type of staff trained
- Statistics on AML training given by authorities to individuals within the businesses/institutions being assessed
- Information on AML training programs and training materials of businesses/institutions within the Other FI category being assessed
- Findings from businesses/institutions (of the Other FI category being assessed) AML on-site/off-site inspections and monitoring
- Interviews/consultations with regulatory/supervisory authorities (e.g., a SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed, including SRBs and professional associations
- Surveys of management and staff from businesses/institutions that make up the Other FI category.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0 ☐	0.9 ☐	0.8 ☐	0.7 ☐	0.6 ☐	0.5 ☐	0.4 ☐	0.3 ☐	0.2 ☐	0.1 ☐	0.0 ☐

4.1.8. Effectiveness of Compliance Function (Organization)

Variable description

This variable assesses whether businesses/institutions within the Other FI category being assessed have effective compliance functions that are comprehensive, risk-based, and well resourced, with independent AML compliance functions.

Assessment criteria

The Other FI category being assessed possesses effective internal AML compliance function if businesses/institutions within the category meet the following criteria:

- Internal compliance programs exist that are commensurate to the level of risk within the businesses/institutions, taking into account important factors (such as the jurisdictions of end-users, professional intermediary clients, clients that are complex, opaque legal structures, the volume and nature of products provided, the client base profile, the frequency of international transactions, etc.).
- A sufficiently resourced, independent AML compliance officer has been appointed and functions at a senior management level.
- Disciplinary actions are taken against staff members in cases of breaches of the compliance policy.
- Internal and/or external AML audits are performed.

Possible sources of information and data

- Relevant regulatory frameworks in relation to compliance function
- Information on internal compliance functions and the policies of businesses/institutions within the Other FI category being assessed
- Findings of the AML on-site inspections and off-site monitoring
- Internal audit reports (and external, if any) on adequacy and effectiveness of compliance functions
- Statistics on disciplinary actions taken by businesses/institutions (of the Other FI category being assessed) against their staff for breaches of the compliance policy
- Statistics on new clients, declined business, or terminated business relationships based on recommendations from the compliance staff
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff from businesses/institutions that make up the Other FI category.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0 ☐	0.9 ☐	0.8 ☐	0.7 ☐	0.6 ☐	0.5 ☐	0.4 ☐	0.3 ☐	0.2 ☐	0.1 ☐	0.0 ☐

4.1.9. Effectiveness of Suspicious Activity Monitoring and Reporting

Variable description

This variable assesses whether businesses/institutions from the Other FI category being assessed have effective and appropriate systems for record keeping, monitoring, and STR reporting to support their AML policies and procedures. A well-designed manual system may be adequate for a small business with a single branch, but large businesses will require more sophisticated systems. A good record-keeping system is a pre-requisite for an effective monitoring system. Any problems and deficiencies in record keeping, therefore, should be assessed under this variable.

Assessment criteria

The businesses/institutions within the Other FI category being assessed have adequate and appropriate AML-monitoring and STR reporting systems if the following criteria are met:

- Firms have information systems that enable and facilitate the monitoring of client transactions and comparisons against the clients' profiles.
- Transactional records are available in a format that facilitates AML screening and monitoring.
- The systems support businesses/institutions in performing effective PEP screening and sanction screening.
- The systems assist businesses/institutions and their staff members in effectively identifying and recording all complex, unusual large transactions.
- The systems assist the businesses/institutions and their staff members in effectively identifying and reporting suspicious transactions.

Staff within the Other FI category should have a good understanding of the scope of their reporting obligations in regard to suspicious transactions and activities, including what activities are covered, or not covered, under laws and regulations.

Possible sources of information and data

- Relevant legal and regulatory frameworks in relation to AML monitoring, record-keeping, and STR reporting obligations within the Other FI category being assessed
- Findings from AML monitoring and supervision with regard to the effectiveness of the STR reporting systems in place in businesses/institutions of the Other FI category being assessed (how many businesses/institutions are compliant, how many are not, and how this impacts the overall effectiveness of STR reporting systems within the Other FI category being assessed).
- Statistics on the number and quality of STRs filed by businesses/institutions (from the Other FI category being assessed), including the number filed "defensively" (after being alerted to suspicious activity or investigation by authorities)
- Statistics on the number of STRs relating to (for example) monitoring lapses that originate from the businesses/institutions within the Other FI category being assessed
- Statistics on the number of STRs filed by businesses/institutions (in the Other FI category being assessed) that have been referred to law enforcement agencies
- Statistics on the number of detected complex and unusual large transactions that were recorded by the reporting entity and not reported
- Information on the quality and accessibility of the transaction and CDD records for the businesses/institutions within the Other FI category
- Findings from businesses/institutions AML on-site/off-site supervision
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff from businesses/institutions that make up the Other FI category.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1	0.0

4.1.10. Availability and Access to Beneficial Ownership Information

Variable description

This variable assesses whether it is easy for criminals to hide their beneficial ownership in corporations, trusts or similar structures registered in or administered from within the country.

Assessment criteria

Transparency relating to beneficial interests in corporations, trusts or similar entities is in place if comprehensive information on the structure, management, control, and beneficial ownership in corporations, trusts and similar vehicles is readily available and can be accessed in a timely manner by competent authorities and is available to AML-regulated institutions and businesses and professions to facilitate their Customer Due Diligence requirements.

**This variable is also assessed by the National Vulnerability and Banking Sector Vulnerability Working Groups. Assessment ratings can be obtained from these Working Groups.*

Possible sources of information and data

- Information as to whether regulated businesses or professions (e.g., lawyers, notaries, or Trust and Company Service providers) are required to form, register, or administer a legal entity or legal arrangement
- Information as to the mechanism chosen by the country to collect and maintain basic and beneficial ownership information of legal entities formed or registered in the country, and beneficial ownership information of legal arrangements formed or administered in or from the country
- The relevant regulatory framework and the effectiveness of beneficial ownership information Customer Due Diligence requirements (pertaining to natural persons and legal entities and legal arrangements)
- Statistics or information on crimes (including money laundering involving the use of shell companies or other opaque structures) and whether accurate, adequate, and current beneficial ownership information can be accessed in a timely manner by competent authorities
- Interviews/consultations with the reporting entities and their supervisory authorities, law enforcement agencies, tax authorities, and, if applicable, the supervisors of Trust and Company Service providers
- Interviews/consultations with Trust and Company Service providers, law firms, and accountancy firms
- Surveys of reporting entities' management and staff
- Experience and opinion of the public authority or private agency that registers corporations and other legal entities.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0 ☐	0.9 ☐	0.8 ☐	0.7 ☐	0.6 ☐	0.5 ☐	0.4 ☐	0.3 ☐	0.2 ☐	0.1 ☐	0.0 ☐

4.1.11. Availability of a Reliable Identification Infrastructure

Variable description

Financial transparency and customer identification and verification processes are enhanced when AML-regulated institutions are able to verify the identity of customers using reliable, independent source documents, data or information. A good identification infrastructure will also prevent the use of fake documents and false identities. Fake documents and false identities hamper the ability to detect and investigate money laundering and trace the proceeds of crime.

Assessment criteria

A good identification infrastructure exists and information is available if AML-regulated institutions can rely on the country's identification infrastructure. For instance, there is reliable and secure government or private sector documentation, data or information to identify and verify the identity of the clients.

The infrastructure may consist of:

- A secure national identification system with government-issued identity documents, whether issued by the national or a local authority, and/or
- Comprehensive and reliable public information systems that assist in the verification of details of clients' details.

**This variable is also assessed by the National Vulnerability and Banking Sector Vulnerability Working Groups. Assessment ratings can be obtained from these Working Groups.*

Possible sources of information and data

- Information about the national identification system
- Information on national identification (ID) infrastructure database and its suitability and availability for ID verification purposes (if available)
- Information on available identification documents and installed anti-counterfeit measures
- Statistics (or experience) concerning the frequency of cases that involve the use of fraudulent ID documents
- Statistics relating to the part of the population that lacks proper ID documents
- Information on any community, social group (such as immigrant communities, tribes, etc.) whose members have no ID documents or have no access to ID documents
- Discussions with reporting institutions on the usefulness of the identification infrastructure
- Discussion of reasons why the national identification system and practices are not working ideally.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0 ☐	0.9 ☐	0.8 ☐	0.7 ☐	0.6 ☐	0.5 ☐	0.4 ☐	0.3 ☐	0.2 ☐	0.1 ☐	0.0 ☐

4.1.12. Availability of Independent Information Sources

Variable description

This variable assesses the availability of independent and reliable sources of information to determine transaction patterns of clients. Customer due diligence processes are easier to perform, and are generally of a higher quality, if such sources are available. They can be used to identify or verify clients' transactional patterns and commercial history. Such information may include data held by credit bureaus, details of previous banking relationships, accessibility to former employers, and the availability of utility bills.

Assessment criteria

Independent and reliable information sources are available if sources of comprehensive and reliable historical financial information and other information about clients are available and can easily be accessed by AML-regulated institutions.

**This variable is also assessed by the National Vulnerability and Banking Sector Vulnerability Working Groups. Assessment ratings can be obtained from these Working Groups.*

Possible sources of information and data

- Interviews/consultations with the reporting entities and their respective supervisory authorities
- Surveys of reporting entities' management and staff
- Interviews with credit bureaus, utility companies, etc., with regard to information available on clients.

Assessment

Based on the assessment criteria and collected information/data, decide the appropriate rating for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0 ☐	0.9 ☐	0.8 ☐	0.7 ☐	0.6 ☐	0.5 ☐	0.4 ☐	0.3 ☐	0.2 ☐	0.1 ☐	0.0 ☐

4.2. Assessment Worksheets for the Inherent Vulnerability Variables

This section provides guidance for the assessment of the inherent factors that are specific to each of the assessed Other FI categories. These factors are called "inherent vulnerability variables". Each assessment worksheet contains a description of the variable, the assessment criteria, a brief guidance on how to support the assessment, and an assessment section to record the decided ratings.

Note: WG can also decide to assess each of the Other FI categories with product-specific input variables. The criteria for assessing these product-specific input variables are the same as the criteria for assessing broader inherent vulnerability factors for the Other FI category as a whole. See Annex 2 for a more detailed product-based assessment.

This section includes guidance about six inherent vulnerability variables.

Inherent vulnerability variables

The following input variables reflect the inherent vulnerability factors:

1. *Total size/volume of the Other FI category*
2. *Client base profile of the Other FI category*
3. *Use of agents in the Other FI category*
4. *Level of cash activity in the Other FI category*
5. *Frequency of international transactions in the Other FI category*
6. *Other vulnerable factors of the Other FI category, including*
    a. *Anonymous use of product in the Other FI category*
    b. *Difficulty in tracing the transaction records*
    c. *Existence of ML typologies on the abuse of the Other FI Category*
    d. *Use of the Other FI category in fraud or tax evasion schemes*
    e. *Non-face-to-face use of product in the Other FI category*
    f. *Other relevant features (specify up to three)*

An important feature that should be considered is whether the same products within the Other FI category can be obtained from unlicensed, and/or unregulated businesses.

These six inherent vulnerability input variables determine the vulnerability for each of the Other FI category being assessed. The assessment of these six inputs should be performed separately for each of the Other FI category being assessed. If the country is assessing 10 Other FI categories, therefore, there are (6*10=) 60 inherent variables that will need to be assessed.

Complete the Entry Page (Vulnerability) tab in the Excel file

The results of the assessments of the inherent vulnerability variables need to be entered into the **Entry Page (Vulnerability)** tab of the Other FI Vulnerability Excel file 6.A/6.B (depending on which assessment type being used). This should only be done after every variable has been assessed. Please refer to Annex 1 for detailed instructions on how to use the Excel file.

4.2.1. Total size/volume of the Other FI category

Determine the total size/volume of the category. The total size/volume for the Other FI category can be measured by using one or more of the three indicators listed below (depending on the nature of the Other FI category being assessed). It is up to the Working Group (WG) to decide which indicators to take into consideration. Ultimately one, or a combination, of the indicators should lead the WG towards an assessment rating for the total size/volume of the Other FI category. The indicators are:

1. A Total Number of Providers (operating in the Other FI category)
1. B Total Asset Size of the Other FI category
1. C Total Turnover of the Other FI category

1.A Total Number of Providers

Variable description

This variable assesses the total number of providers (the businesses/institutions) that make up the Other FI category, which is indicative of the level of ML vulnerability that they can introduce into the Other FI category (if the relevant risks are not mitigated).
For some categories (especially unregulated ones), the actual number of providers may be difficult to determine. In that case, a judgment is required as to whether the providers are significant to the country's economy.

Assessment criteria

The objective of this indicator is to assess the importance of the Other FI category within a country's economy (compared to the other sectors that are being assessed).

The most appropriate indicator of the total number of providers within the Other FI category depends on the nature of the products being provided. In other words, if a country licenses an FI category, but unlicensed businesses provide the same services, efforts should be made to ascertain (even if only an estimate) the number of both licensed and unlicensed providers. For example, in some countries, money remittance services may not only be provided by large money remittance organizations, but also by more informal remittance providers who are unlicensed and tend to operate outside the regulated financial system.

For certain Other FI categories, the number of providers is a good indicator to use, because even if the value of the products is relatively small, the presence of a high number of providers is reflective of the work regulators and supervisors need to put in to ensure that all business providers comply with AML requirements.

Possible sources of information and data

- Data on the total number of providers (businesses/institutions, both licensed and unlicensed) within the Other FI category being assessed
- Interviews/consultations with regulatory/supervisory authorities (e.g., a Self-Regulatory Body [SRB]), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff from businesses/institutions that make up the Other FI category
- Interviews with, and data compiled by, private sector research or consulting firms.

Additional guidance

Also consider whether the particular product can only be provided in the jurisdiction by licensed businesses/institutions, or
(1) Is permitted to be provided by "informal" or unlicensed businesses/institutions, and/or
(2) Is not permitted within the jurisdiction, but the product is being provided by "informal" or unlicensed businesses/institutions (because of a lack of clarity within the laws/regulations, or a lack of effective enforcement against unlicensed businesses/institutions).

While assessing the total number of providers, try to decide whether it is significant or not. If it is significant, rate it as high; if not significant, rate it as low. If you think that it is moderately significant, rate it as medium.

1. B Total Asset Size of the Other FI Category

Variable description

This variable assesses the size of the total assets with the Other FI category. Total asset size may be indicative of the level of ML vulnerability that can be introduced into the Other FI category (if the relevant risks are not mitigated).

In the cases where the total asset size of the Other FI category is difficult to determine, the assessment may require a judgment as to whether the total assets held by the Other FI category is significant within the country's economy.

Total asset size may be a meaningful indicator for some Other FI categories (especially non-bank credit institutions), but not for others. The asset size should, therefore, only be taken into account if it is meaningful.

Assessment criteria

The objective of this indicator is to assess the importance of the Other FI category in comparison to the other sectors being assessed.

The most appropriate indicator of the total asset size within the category depends on the nature of the products being provided by the Other FI category. For example, consider the services offered by leasing, and factoring institutions: the total asset size of that particular category may be greater than when compared with another FI category.

Possible sources of information and data

- Data on the total assets and liabilities associated with the Other FI category being assessed
- Data on the total assets managed that are associated with the product of the Other FI category being assessed
- Interviews/consultations with regulatory/supervisory authorities (e.g., a SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff from businesses/institutions that make up the Other FI category
- Interviews with, and data compiled by, private sector research or consulting firms.

Additional guidance

While assessing the total asset size of the Other FI category, decide whether it is significant or not. If it is significant, rate it as high; if not significant, rate it as low. If you think that it is moderately significant, rate it as medium.

1. C Total Turnover/Value of the Other FI Category

Variable description

This variable assesses the total turnover, or total value/amount, of transactions handled by a particular Other FI category. Total turnover may be indicative of the level of ML vulnerability within the category (if the relevant risks are not mitigated).

When the total turnover of the Other FI category is difficult to determine, the assessment may require a judgment as to whether the total turnover of the Other FI category being assessed is significant to the country's economy.

Assessment criteria

The objective of this indicator is to assess the importance of a particular Other FI category within a country's economy (compared to the other sectors being assessed).

For some categories, such as money remittance organizations or exchange bureaus, turnover (i.e., the total value of the transactions they are handling) is a more meaningful indicator than asset size. Besides the financial statements and tax records of a country, the Other FI category's contribution to GDP may provide useful information about this indicator.

However, turnover/value can be a more accurate indicator than total assets. This is because, in some categories (e.g., money transfer services and exchange bureaus) there are few assets although large volumes of transactions, in large sums, are processed, all of which delivers a high turnover. Besides financial statements and tax records, therefore, the category's contribution to the national GDP is also a good indicator.

Possible sources of information and data

- Data on the total value of transactions associated with the Other FI category being assessed
- Data on the total turnover associated with the Other FI category being assessed
- Data on the total amount of fund flows associated with the Other FI category being assessed
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of managements and staff from businesses/institutions that make up the Other FI category
- Interviews with, and data compiled by, private sector research or consulting firms.

Additional guidance

During the assessment, the WG needs to refer to both official data and the best available estimates from reliable sources. While assessing the total turnover/value of the Other FI category, decide whether it is significant or not. If it is significant, rate it as high; if not significant, rate it as low. If you think that it is moderately significant, rate it as medium.

4.2.2. Client base profile of the Other FI category

Variable description

This variable assesses whether the type of client that generally uses the Other FI category being assessed increases the risk of money laundering abuse within the category.

Note that the term "client" may refer to natural persons, legal persons, or legal arrangements. It may also refer to end-users of the businesses/institutions that make up the Other FI category, or professional intermediary firms through which products are provided to end-users. All forms of clients should be considered within this assessment.

Assessment criteria

The client base profile of the Other FI category should be assessed to carry a higher risk if it involves:

- Domestic and/or international Politically Exposed Persons (PEPs)
- High-net-worth individuals
- Non-resident clients, particularly from high-risk jurisdictions
- Clients with foreign business or personal interests
- Clients with criminal records or past administrative and/or supervisory actions against them
- Clients with business links to known high-risk jurisdictions
- Clients that are legal entities, or arrangements, with complex and opaque ownership and control structures (including layered ownership and control, spanning multiple jurisdictions, or involving high-risk jurisdictions)
- Clients obtained through introduced business, particularly from unregulated professional intermediaries/regulated intermediaries in jurisdictions with low AML controls
- Professional intermediaries in jurisdictions with low, or nonexistent, CDD requirements.

Possible sources of information and data

- Regulatory framework for risk-based classification of clients
- Regulatory framework for identifying and monitoring foreign and domestic PEPs
- Any category-wide statistics on PEPs, and other high-risk clients
- Data on the jurisdictions of origin of end-user clients and professional intermediary firms
- Financial sector data on transactions with high-risk jurisdictions
- Data on clients obtained through introduced business
- Criminal data, including typologies on high-risk clients, and cases where the Other FI category being assessed was used for ML by high-risk clients
- Statistics and information on STRs originating from the Other FI category being assessed, with regard to high-risk clients
- Interviews/consultations with regulatory/supervisory authorities (e.g., a SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff from businesses/institutions that make up the Other FI category
- Interviews with, and data compiled by, private sector research or consulting firms.

Additional guidance

While assessing the client base profile for each of the Other FI categories being assessed, assess whether the products of the Other FI category are being used by the clients who pose the highest money laundering risk, when compared to standard clients. These high-risk clients will include PEPs, non-residents, high-net-worth individuals, among others.

It would be useful to look at the geographical breakdown of the clients and their transactions, including those categorized as high-risk jurisdictions. Many financial institutions categorize transactions based on high-risk jurisdictions as "higher risk" for the purpose of screening and monitoring the transactions and to identify suspicious transactions. Clients and transactions associated with high-risk jurisdictions are likely to be more vulnerable to money laundering, as adequate AML controls are not likely to be in place, and consequently it is easier to move illicit funds to, and from, these jurisdictions into the global financial system.

To assess this variable, Other FI categories should be required to put in place appropriate mechanisms to identify and monitor high-risk individuals (including PEPs). If such monitoring/analysis mechanisms are not in place, the Other FI categories may not be able to provide any information.

While assessing this indicator, question how likely it is that the Other FI category being assessed will be abused by criminals, when compared to Other FI categories. If the likelihood is high, the assessment rating for the client base profile for the Other FI category being assessed should be high.

Assessment of this indicator will require judgment if a country does not have appropriate mechanisms to identify and monitor high-risk clients. If there is no data that can support the assessment, the WG should work on the basis of the worst-case scenario and be conservative in their assessment.

Furthermore, an assessment should be made on how much information is collected by businesses (in relation to their client profile).

One of the choices for this variable within the Excel file is “Not Analyzed.” Note that the Excel file penalizes this, since the lack of ability to analyze the client base profile will pose a risk in itself.

4.2.3. Use of agents in the Other FI category

Variable description

This variable assesses how frequently agents are used to deliver products within the Other FI categories. The ML vulnerability of the category may be increased due to the weak AML systems of agents (including weak systems of the countries in which they operate).

Assessment criteria

The objective of this assessment is to compare the use of agents by the Other FI category being assessed, compared with the use of agents in other FIs.

The use of agents in providing products for Other FI categories should be treated as if it were an extension of the activity of principal financial institution. The greater the use of agents, the higher the risks associated with the Other FI category.

This is because even though agents may be permitted, in effect or practice, to perform identification and verification obligations, the prevalent rule is that principal financial institutions hold, and are accountable for, the business relationship, and are ultimately liable for the compliance of the agents to AML/CFT requirements. Any transaction monitoring systems ought to cover what is performed by the agents.

Possible sources of information and data

- Data on the total number of agents (where agents are licensed/regulated) providing a particular product in the Other FI category being assessed
- Lists of agents maintained by the principle businesses in the Other FI category being assessed
- Data/information on the type of agents providing a particular product within the Other FI category being assessed
- Interviews/consultations with the principle financial institutions, on the use of agents within the Other FI category being assessed
- Interviews/consultations with agents providing products in the Other FI category being assessed
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities; this includes any information gathered from on-site visits to agents
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff from businesses/institutions that make up the Other FI category
- Interviews with, and data compiled by, private sector research or consulting firms
- Criminal data, including ML cases where a product was used for ML due to the activities of an agent in the Other FI category being assessed
- Statistics on STRs (involving the use of agents in the Other FI category being assessed).

Additional guidance

To limit the vulnerability, the agents, or professional intermediaries, have to be subject to adequate AML controls and monitoring/supervision by the principal financial institution providing the product. Consider to what extent agents are supervised and monitored by the principal financial institution for the delivery of the product in the Other FI category being assessed.

The national practices for licensing, registration, or supervision of these agents can differ significantly. It is also important to be aware of the potential practical limitations faced by some type of agents, such as small retailers (for example, mobile money agents are often small shops). Consider their ability to carry out adequate identification and verification of customer information.

4.2.4. Level of cash activity in the Other FI category

Variable description
This variable assesses the level of cash activity associated with the Other FI category being assessed, in particular, whether the use of cash is permitted, and to what extent the use of cash occurs.
Assessment criteria
Assess whether the use of cash is permitted for the Other FI category being assessed, and the level of cash associated with it. The more the Other FI category being assessed is cash-based, the greater its vulnerability to money laundering is.
Possible sources of information and data
• Criminal data, including cases where the Other FI category being assessed was used for ML due to the possibility of using cash transactions (including payment of fees for services provided) • Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities • Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations) • Surveys of management and staff from businesses/institutions that make up the Other FI category • Interviews with, and data compiled by, private sector research or consulting firms.
Additional guidance
When assessing the level of cash activity, consider what is permissible, not just in terms of the amount of cash, but also the denominations typically used in the cash transactions and how frequently cash transactions are carried out. For example, services (such as foreign exchange bureaus) will conduct the greater part of their business in cash transactions, compared to other FI categories. When considering the level of cash activity for a particular Other FI category, consider to what extent the Other FI category may contribute to the informal economy in the country. Are there unlicensed/unregulated businesses that provide some of the products of the Other FI category (e.g., businesses providing informal money remittance services)?

4.2.5. Frequency of international transactions in the Other FI category

Variable description

This variable assesses the frequency of international transactions associated with the Other FI category that could increase the risk of money laundering abuse in that particular Other FI category.

Assessment criteria

Consider if the products of the Other FI category involve international wire transfers and other international transactions. The higher the number of international transactions within the Other FI category, the more vulnerable the Other FI category is to ML.

When assessing this indicator, it is useful to consider the number of correspondent accounts within the Other FI category. This includes the correspondent accounts of the foreign financial institutions held by domestic institutions, and vice versa.

The nature of the transactions, and the jurisdiction breakdown for inward and outward transactions, may provide useful information when assessing the ML risk.

Possible sources of information and data

- Other FI data on international transactions (organized by product/service/category), sorted by jurisdiction breakdown, etc.
- Data on the number of STRs filed in respect to the products provided by Other FI category being assessed
- Criminal data, including cases in which the Other FI category was used for ML and involved in international transactions
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities,
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff from businesses/institutions that make up the Other FI category
- Interviews with, and data compiled by, private sector research or consulting firms.

Additional guidance

Data on international transactions relating to various products provided by Other FI categories should preferably be on a consolidated basis, taking into account data from all providers within the Other FI category.

Also consider if informal providers are engaging in international wire transfers (for example, the existence of informal money remittance providers).

4.2.6. Other vulnerable factors of the Other FI category

Variable description

This variable assesses whether there are any additional factors that render the Other FI category vulnerable to the risk of money laundering.

Assessment criteria

The presence of the following typical factors may increase the ML vulnerability of the Other FI category being assessed:

- Anonymous use of the product in the Other FI category
- Difficulty in tracing the transaction records
- Existence of ML typologies on the abuse of the Other FI category
- Use of the Other FI category in fraud or tax evasion schemes
- Non-face-to-face use of the products in the Other FI category

For all of the above factors, consider whether there is also an international dimension, and how that may increase the vulnerability of the Other FI category to ML risk.

Possible sources of information and data

- Criminal data, including cases in which the Other FI category being assessed was used for ML, indicating vulnerability due to the above-mentioned factors
- Data/statistics/qualitative information from MLA and formal or informal information/intelligence sharing requests from supervisory authorities, law enforcement, the FIU, tax authorities, and other relevant authorities
- Interviews/consultations with regulatory/supervisory authorities (e.g., an SRB), or other competent authorities
- Interviews/consultations with representatives from the Other FI category being assessed (including SRBs and professional associations)
- Surveys of management and staff from businesses/institutions that make up the Other FI category
- Interviews with, and data compiled by, private sector research or consulting firms.

Additional guidance

Please note that that existence of one or more of these factors may render a business/profession vulnerable to money laundering.

Anonymous use of the product in the Other FI category:

Assess whether anonymous use of the product is possible for the Other FI category being assessed. Consider whether the beneficial owner of the transaction is always identified and verified. Does the Other FI category allow for anonymous use of its products (where a firm or an individual known to a business uses the products on behalf of several firms – or individuals – that are unknown to the business?). Anonymous transactions are vulnerable to money laundering as the beneficial owner(s) of the funds involved in the transaction is not known or unverified. The transaction is executed for the client on behalf of others. The real owners are not known, and hence not subject to Customer Due Diligence.

Difficulty in tracing the transaction records: Assess whether the transactions executed over the course of the delivery of a product from the Other FI category are properly recorded and whether access to those records can be readily obtained for CDD/EDD. The difficulty in tracing records depends on the quality of the AML, CDD, and record-keeping systems of the Other FI category being assessed.

Existence of ML typologies on the abuse of the Other FI category: If the Other FI category is known for ML abuse, this can raise ML vulnerability. This does not necessarily need to be country-specific. Consider the typologies at a global level, regardless of whether it was detected within the country or not.

Use of the Other FI category in fraud, or tax evasion, schemes: Assess the use of the Other FI category in fraud/tax evasion, schemes, or other predicate offenses. It may be useful to refer to crime and tax enforcement data in order to find the Other FI categories that are most vulnerable to actual and potential misuse. Additionally, the use of the Other FI category in tax evasion, fraud schemes, or other predicate offenses may indicate a vulnerability to ML abuse.

Non-face-to-face use of the product in the Other FI category: Availability of non-face-to-face initiation of business relationships, with respect to the Other FI category (or product), raises ML vulnerability. If, for example, an individual is able to secure the product via the Internet or telephone with non-face-to-face contact with the business, there is ML vulnerability. Even in the case where non-face-to-face initiation of a product is not allowed, but non-face-to-face use of the product is, there is a possibility of ML vulnerability. But in the second case, the vulnerability of the product can be less, depending on the quality of CDD done during the face-to-face product initiation and existence of other controls that limit the use of the product by persons other than the client end user.

Any other vulnerable factors: Consider any other specific factor(s) that may render the Other FI category vulnerable to money laundering.

Summary of the assessment of the Other FI category: Considering the assessment criteria and guidance, assess the inherent vulnerability variables associated with the assessed Other FI category. For each of the assessed Other FI categories, check (✓) the appropriate option in the table. Repeat this for each of the Other FI category being assessed.			Other FI category (Module 6.A) Product 1 (Module 6.B)	Product 2 (Module 6.B)	Product 3(Module 6.B)	Product 4(Module 6.B)	Product 5(Module 6.B)
(A, B, C) ***Total size/volume of the Other FI category***		High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Not Analyzed					
Client base profile of the Other FI category		Very High Risk					
		High Risk					
		Medium Risk					
		Low Risk					
		Very Low Risk					
		Not Analyzed					
Use of agents in the Other FI category		High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					
Level of cash activity in the Other FI category		High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					
Frequency of international transactions in the Other FI category		High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					
Other vulnerable factors of the Other FI category	Anonymous use of the product	Available					
		Not Available					
	Difficulty in tracing transaction records	Records not available					
		Difficult/Time Consuming					
		Easy to trace					
	Existence of ML typologies on the abuse of the Other FI category	Exist and Significant					
		Exist					
		Exist but Limited					
		Does Not Exist					
	Use of the Other FI category in fraud or tax evasion schemes	Exist and Significant					
		Exist					
		Exist but Limited					
		Does Not Exist					
	Non-face-to-face use of product in the Other FI category	Available and Prominent					
		Available					
		Available but Limited					
		Not Available					

Summary of the assessment of the Other FI category: Considering the assessment criteria and guidance, assess the inherent vulnerability variables associated with the assessed Other FI category. For each of the assessed Other FI categories, check (✓) the appropriate option in the table. Repeat this for each of the Other FI category being assessed.			Other FI category (Module 6.A) Product 1 (Module 6.B)	Product 2 (Module 6.B)	Product 3(Module 6.B)	Product 4(Module 6.B)	Product 5(Module 6.B)
	Other factors (specify)	High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					
	Other factors (specify)	High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					
	Other factors (specify)	High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					

In case of a product-based assessment of the Other FI category, please assess the inherent vulnerability variables associated with each product within the Other FI category being assessed. Repeat the assessment for all the assessed Other FI categories. Refer to Annex 2 for more details.

5. DESCRIPTION OF THE INTERMEDIATE VARIABLES

(Ranging from lower level intermediate variables to higher level variables – Cf. Figure 3.a)

VARIABLE	DESCRIPTION
Quality of AML Supervision	This variable assesses whether the Other FI category being assessed has a comprehensive AML supervision regime supported by appropriate powers, staff, and other resources. This variable depends on the: • *Effectiveness of Supervision/Oversight Activities* • *Availability and Enforcement of Administrative Sanctions*.
Commitment and Leadership of Managements	This variable assesses the commitment and leadership in AML of the management of the businesses/institutions (of the Other FI category being assessed), and how managements are influenced by the following variables: • *Availability and Effectiveness of Entry Controls* • *Quality of AML Supervision* (intermediate variable) • *Availability and Enforcement of Criminal Sanctions*.
Quality of AML Policies and Procedures	This variable assesses the quality of the internal AML policies and compliance procedures in the businesses/institutions within the Other FI category being assessed, which depends on the: • *Comprehensiveness of the AML Legal Framework* • *Commitment and Leadership of Managements* (intermediate variable) • *Effectiveness of Compliance Functions*.
Compliance Level of Staff	This variable assesses the compliance levels of staff in the businesses/institutions (of the Other FI category being assessed) with regard to AML legal framework and their institutional obligations. This variable considers how this is influenced by factors such as the: • *Availability and Enforcement of Criminal Sanctions* • *Effectiveness of Compliance Functions*, • *AML Knowledge of Businesses/Institution Staff* • *Integrity of Businesses/Institution Staff*.
Quality of CDD Framework	This variable assesses whether the country has the legal, institutional, and technical framework to identify and verify the identities of natural and legal persons, to store the identification records, and to facilitate the use of this information by authorized parties for AML purposes. This variable depends on the: • *Availability and Access to Beneficial Ownership Information* • *Availability of a Reliable Identification Infrastructure* • *Availability of Independent Information Sources*.
Quality of Operations	This variable assesses the quality of operations within the businesses/institutions in preventing the abuse of the Other FI category being assessed for money laundering. This variable depends on the: • *Commitment and Leadership of Managements* (intermediate variable) • *Compliance Level of Staff* (intermediate variable), • *Quality of CDD Framework* (intermediate variable) • *Effectiveness of Suspicious Activity Monitoring and Reporting*.

VARIABLE	DESCRIPTION
Quality of AML Controls	This variable assesses the quality of AML controls within the Other FI category being assessed, which are the standard AML controls that apply to the category as a whole, or to all of its products. This variable depends on the: • *Quality of AML Policies and Procedures* (intermediate variable) • *Quality of Operations* (intermediate variable).
Inherent Vulnerability for Other FI category ***Product Inherent Vulnerability*** **(applicable for product-based assessment only)**	This variable assesses the susceptibility of the Other FI category being assessed as a whole, or the susceptibility of its product to money laundering, solely based on key inherent factors of the category (or its products), without taking into account its AML controls. The Other FI category (or its product) being assessed is inherently vulnerable when its characteristics render it open to abuse for money laundering. This relies on inherent vulnerability variables, namely: • *Total size/volume of the Other FI category* (or product) • *Client base profile of the Other FI category* (or product) • *Use of agents in the Other FI category* (or product) • *Level of cash activity in the Other FI category* (or product) • *Frequency of international transactions in the Other FI category* (or product) • *Other vulnerability factors of the Other FI category* (or product).
(Overall) *Product Vulnerability* **(applicable for product-based assessment only)**	This variable assesses the overall susceptibility of a particular Other FI category's product to money laundering given its inherent vulnerability and the AML control mechanisms put in place to address that vulnerability. The more susceptible the product is, the more money laundering transactions can occur undetected. This variable depends on the: • *Inherent Vulnerability of the Product* (intermediate variable) • *Quality of AML Controls* (intermediate variable). **The ratings of all the product vulnerability assessments (of the Other FI category being assessed) determine the final vulnerability of the Other FI category being assessed.**
Other FI Category Final Vulnerability	This variable assesses the overall vulnerability of a particular Other FI category being assessed to money laundering. The final vulnerability of the Other FI category depends on the: • *Inherent Vulnerability for the Other FI category* • *Quality of AML Controls*.

ANNEX 1 – INSTRUCTIONS FOR USING THE EXCEL FILE

At this stage, the input variables have been assessed, and assigned a rating. These ratings now need to be entered into the Excel file. This Annex provides step-by-step instructions for using the Excel files (6.A/6.B) to assess the vulnerabilities of the Other FI categories.

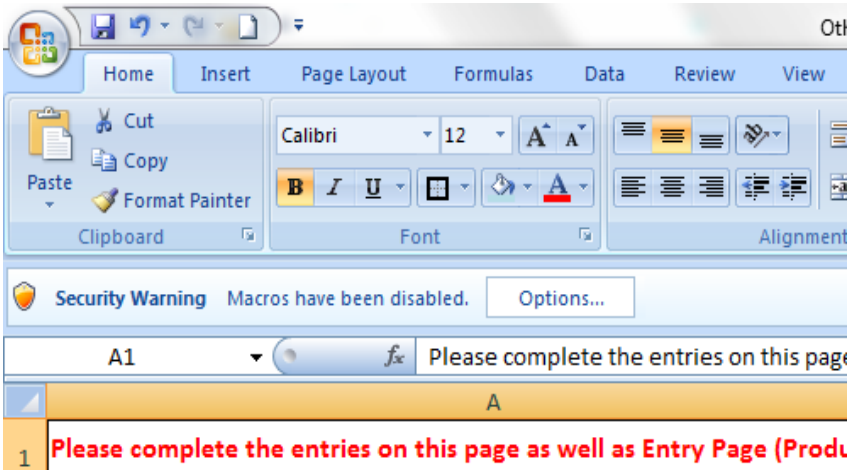
The WG should use Excel File 6.A if assessment is undertaken without detailed product assessment. In case of a product-based assessment, use Excel File 6.B.

- While reading these instructions, open and try to use the Excel file in parallel to aid your understanding.
- Please make sure that you have a recent and full version of Windows Office Excel installed. The Excel file works only with Office Professional 2007 and later versions. Earlier versions or home/student versions of Excel, which have limited functions, do not support the file.
- Do not work in the original Excel file. Always create a copy of it and work in the copied (working) version. This way, if the macros in the working version become corrupted, you will still have an intact version of the file.
- Do not add or delete any rows/columns in the Excel file, as this can corrupt the macros or formulas in it.

Step 1: Before you start

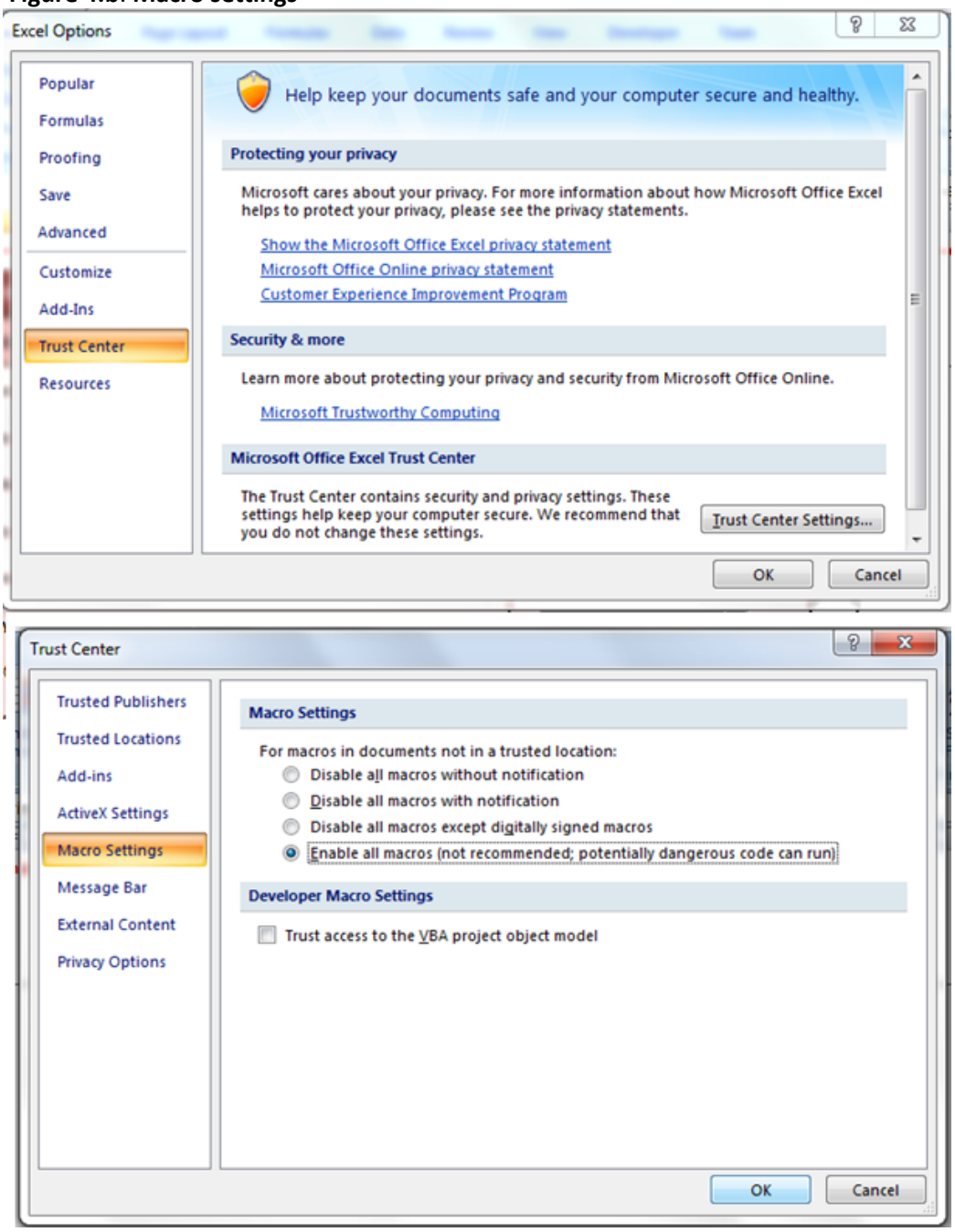
After opening the Excel file, first enable macros. A security warning will appear in the top left-hand corner of the first tab (Entry Page), warning you that macros are disabled – as shown in Figure 4.a. Click on the **Options** icon and select the **Enable this Content** option. Click **OK**, or (depending on which version of Excel is being used) click on the **Enable Content** icon in the toolbar. This is an important step, because without it the Excel file will not function properly.

Figure 4.a: Macro security warning



If the macro security warning (Figure 4.a) does not appear, change the macro settings. To change the macro settings, click the **Microsoft Office Button** (in the top left corner) and select **Excel Options**. In the Excel Options window, select the **Trust Center** option and click on **Trust Center Settings** (see Figure 4.b). When the Trust Center window opens, select the **Macro Settings** option (Figure 4.b). In this list, select the option **Enable all Macros** and click **OK**.

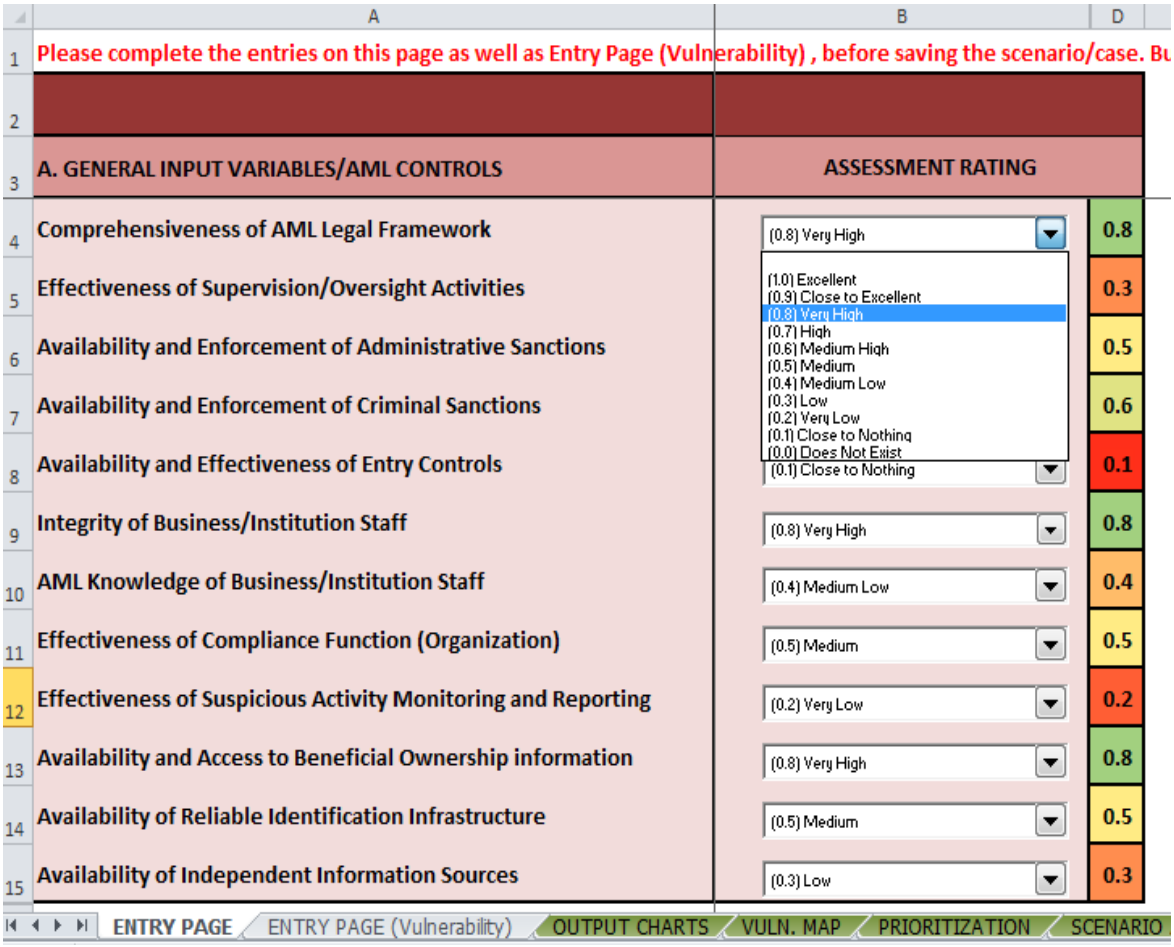
Figure 4.b: **Macro settings**



Step 2: Entries for general input variables (in the Entry Page tab)

For each general input variable, select your chosen rating in the drop-down list. The options range from **(1.0) Excellent** to **(0.0) Does Not Exist**. Notice that higher assessment ratings for general input variables implies that the country has better AML controls in place, which will lead to a lower overall vulnerability for the assessed Other FI category. The Excel file automatically colors the entries according to their level of desirability (i.e., green = desirable, red = undesirable, etc.) – as shown in Figure 5. For both the excel files (6.A and 6.B), the Entry (page) tab is similar.

Figure 5: **Entries for general input variables (in the Entry Page tab (applicable to both Excel files, 6.A and 6.B)**



To complete the assessment, assessment ratings need to be entered for all twelve general input variables.

Bear in mind that the assessment of the general input variables is applicable to the assessed Other FI category as a whole, and will influence the vulnerabilities of all the businesses and institutions operating within the assessed Other FI category. In case of product-based assessment (Excel file 6.B), it will also

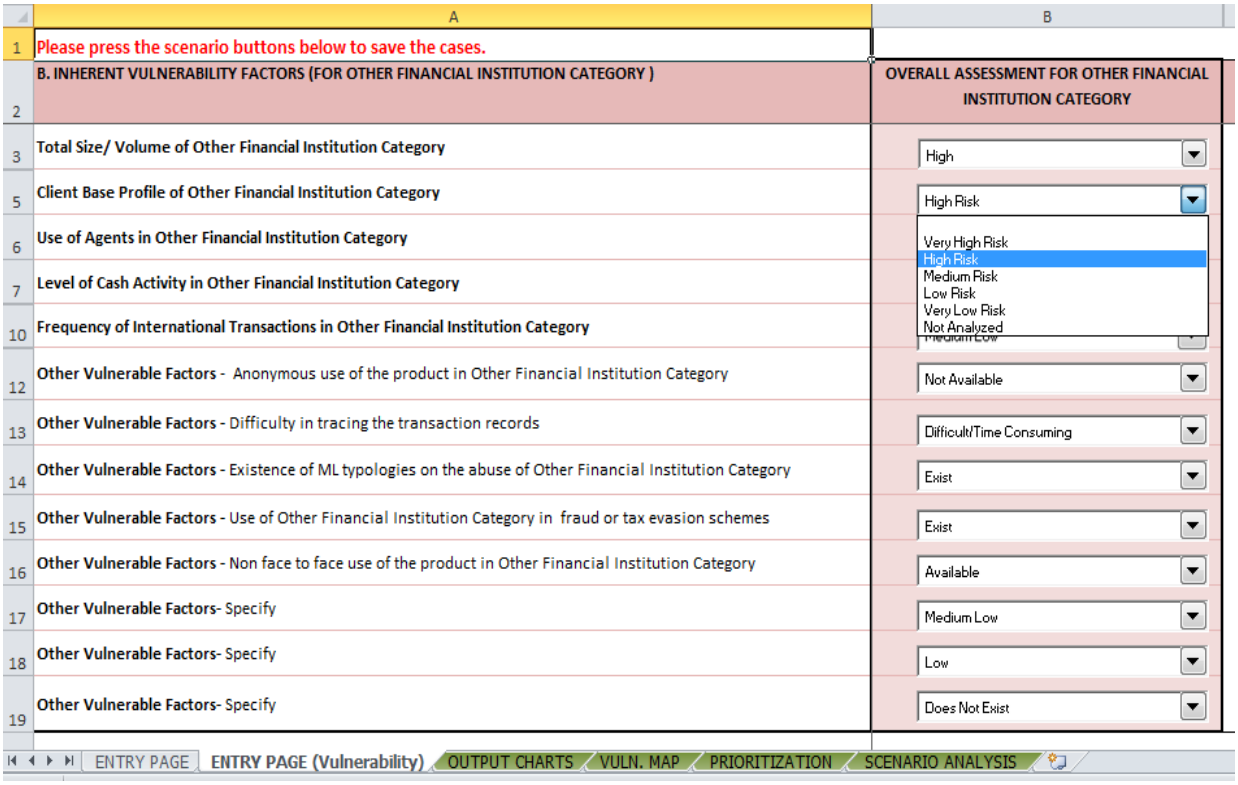
influence the vulnerabilities of all the products offered by the businesses and institutions operating within the assessed Other FI category.

Step 3: Entries for inherent vulnerability variables (in the Entry Page (Vulnerability) tab)

Once all the general input variables assessment ratings have been entered into the Entry Page tab, move to the next tab, which is Entry Page (Vulnerability). This is where the entries for inherent vulnerability factors for the assessed Other FI category are entered. During the assessment, you will decide which types of Other FI categories to include. Use separate excel files for each type of Other FI category to be assessed.

Enter the assessment ratings for each of the inherent vulnerability variables related to the assessed Other FI category by clicking on the drop-down list in column B (see Figure 6).

Figure 6: Entries for inherent vulnerability variables (in the Entry Page (Vulnerability) tab) (Excel File 6.A)



If the rating for any inherent vulnerability variable has not been entered, a warning that the file is incomplete will appear in row 20 of the Entry Page (Vulnerability) tab.

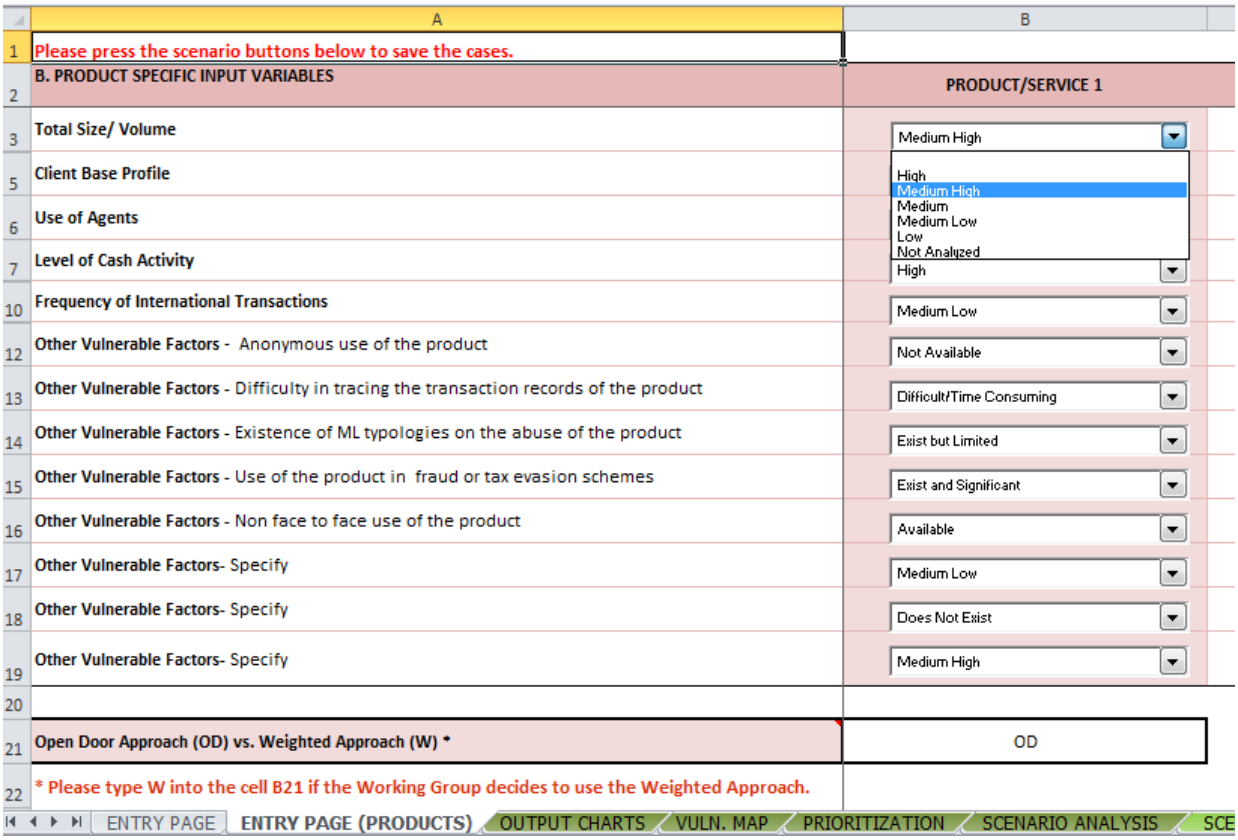
Step 3: Entries for inherent vulnerability variables (in the Entry Page (Products) tab) (applicable in case of product-based assessment, Excel File 6.B)

Once all the general input variables assessment ratings have been entered into the Entry Page tab, move to the next tab, which is Entry Page (Products). This is where the entries for product-specific input variables are entered. During the assessment, you will decide which products to include. The design of the Excel file allows you to change the names of the products. The names of the products that are to be assessed should be inserted in row 2. Click on the cells that read Product/Service #, and enter the name of the product to be assessed. Please note that product based assessment is undertaken for a specific Other FI category.

Enter the assessment ratings for each of the specific input variables by clicking on the drop-down list in column B/column C, respectively for each of the products. In this tab, the specific input variables (column A) will be assessed for each of the selected products for the assessed Other FI category (see Figure 7).

The Excel file is designed to facilitate the assessment of up to 5 products. However, if needed, you can use a second file to assess additional products. In this case, to assess the vulnerability of the Other FI category, the Working Group should use a third file as the master file. This master file should include only the 5 products with the highest vulnerability in two working files.

Figure 7: Entries for product-specific input variables (in the Entry Page (Products) tab) (Excel File 6.B)



If the rating for any specific input variable has not been entered for a product, a warning that the file is incomplete will appear in row 20 of the Entry Page (Products) tab.

The Working Group may choose one of two approaches in assessing the impact of a given product's vulnerability to money laundering:

(1) The Weighted Average Approach. This straightforward approach calculates the overall vulnerability of the assessed Other FI category on the basis of the weighted averages of all the products assessed. Weights are determined by the total size/volume entries of each of the assessed products.

(2) The Open Door Approach. This approach calculates the vulnerability score of the assessed Other FI category, not by focusing on weighted averages of products but rather on those products that are most vulnerable. It can perhaps best be illustrated by using the metaphor of a house. Suppose a building has ten doors (products), one of which is open. Using the Weighted Average Approach, the overall vulnerability of the building would end up as relatively low (10 percent). However, in practice, we know that one open door may make the building highly vulnerable. To take account of this, therefore, in determining vulnerability, the Open Door Approach focuses on the products with higher vulnerability.

The Open Door Approach has been chosen as the default option in the Excel file 6.B. Thus, the entry in cell B 21 is "OD" (see Figure 7). If you prefer the Weighted Average Approach, switch to the weighted average option by entering "W" in this cell.

In order to compare the outcomes of the two approaches, it is suggested that the Working Group try the Open Door Approach first and then try the Weighted Average Approach, working as follows. First, make the assessment using the Open Door Approach and save the file. Then create a copy of this file and change the option from "OD" to "W" in cell B 21, as discussed above. Save this file under another name. Compare the overall vulnerability of the assessed Other FI category using each option and decide which results make more sense. Whichever approach and result is finally chosen, the outcome must be supported with documentation of the underlying argument.

Step 4: Saving the entries

After the results for the input variables (step 2 and step 3) have been entered, save the entries by clicking the **Save the Original Case** icon on the Entry Page (Vulnerability) tab- as shown in Figure 8 or Entry Page (Products) tab – as shown in Figure 9 **(Applicable in case of product based assessment – Excel file 6.B)**. This is an important step as the case needs to be saved before you can proceed. Otherwise, the output charts will not show the results of the assessment. (Bear in mind that this saves only your entries, not the file. You still have to save the Excel file to not lose your data.)

Figure 8: Icons on the Entry Page (Vulnerability) tab (Excel File 6.A)

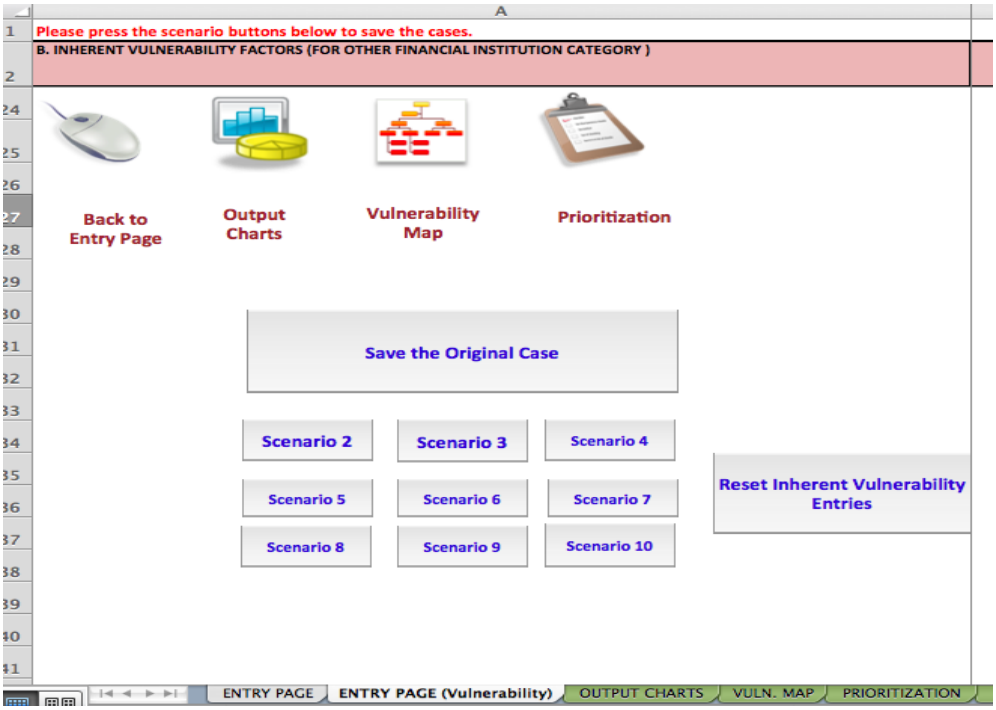
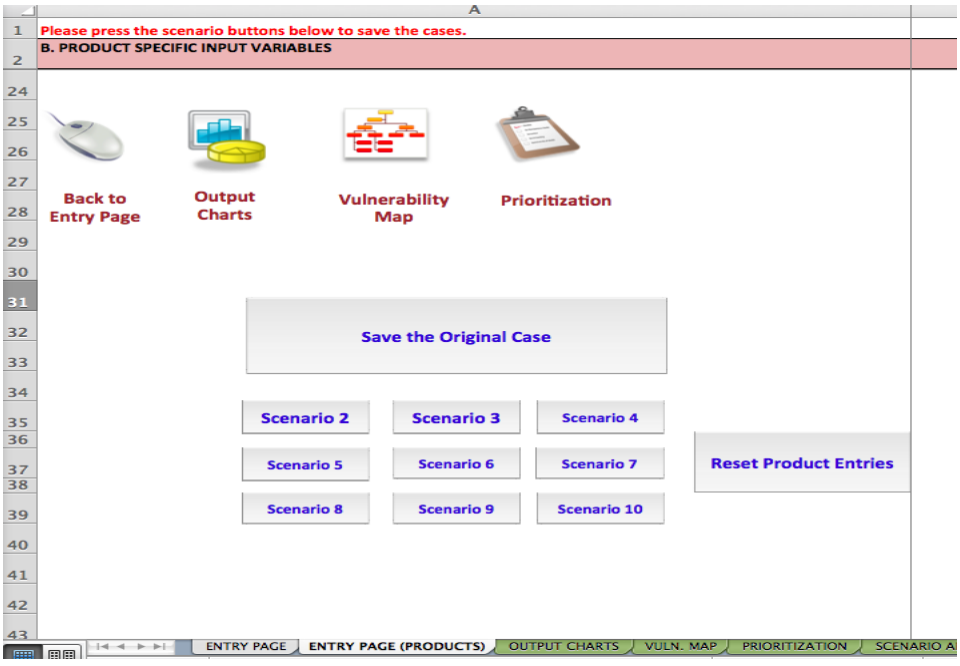


Figure 9: Icons on the Entry Page (Products) tab (applicable in case of product based assessment, Excel File 6.B)



Step 5: The outputs of the assessment

After the case has been saved, the Excel file automatically generates the outputs of the assessment. There are three outputs, which are captured in three separate tabs:

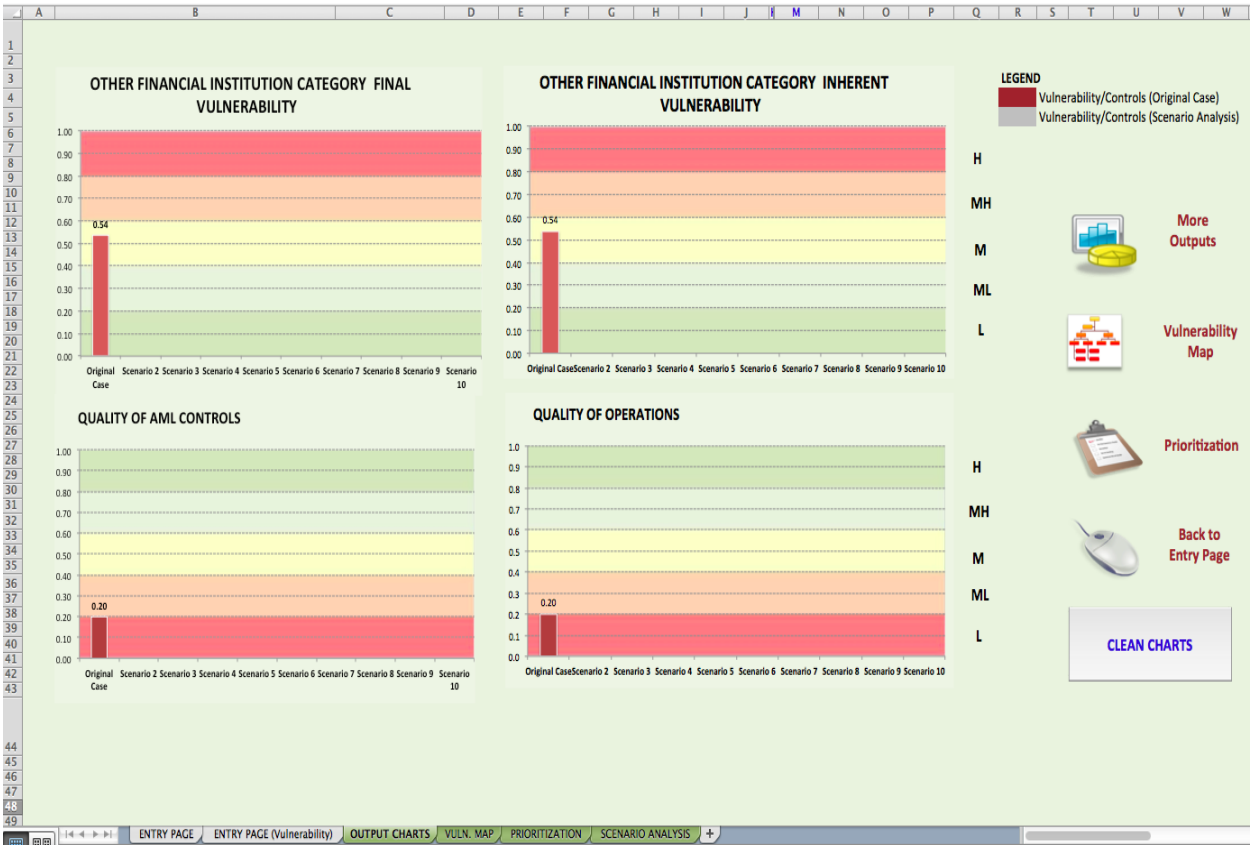
(1) Output Charts
(2) Vulnerability Map (Network Diagram)
(3) Prioritization.

(1) Output Charts tab

The Output Charts tab shows the final and inherent vulnerability score of the assessed Other FI category, and the assessment results for intermediate variables such as *Quality of AML Controls,* in a visual format (see Figure 10). For output charts, click on the **Output Charts** icon in the Entry Page (Vulnerability) tab to view the assessment results (as shown in Figure 8).

The inherent vulnerability score of the assessed Other FI category does not take into account the impact of AML controls on the vulnerability of the Other FI category. On the other hand, the final vulnerability score is calculated after taking into account the impact of AML controls. The more effective and comprehensive the AML controls, the lower the final vulnerability of the assessed Other FI category.

Figure 10: Output charts (Excel File 6.A)



For both the vulnerability charts, a higher score implies a higher vulnerability to ML. On the other hand, for intermediate variables that relate to controls (such as *Quality of AML Controls, Quality of CDD Framework*, and *Quality of Operations*) a higher score indicates a higher combating ability, which lowers the vulnerability of the assessed Other FI category to ML.

Output Charts tab – For Product-based Assessment (Excel File 6.B)

The Output Charts tab shows the final vulnerability of the assessed Other FI category, the vulnerability of each assessed product for the Other FI category, and the assessment results for intermediate variables such as *Quality of AML Controls,* in a visual format (see Figure 11.a and Figure 11.b). For output charts, click on the **Output Charts** icon in the Entry Page (Products) tab to view the assessment results (as shown in Figure 9).

The product vulnerability chart shows both the inherent vulnerability scores (light blue bar) and the final vulnerability scores (dark blue bar) of each product assessed. The inherent vulnerability score does not take into account the impact of AML controls on the vulnerability of a product. On the other hand, the final vulnerability score is calculated after taking into account the impact of AML controls. The more effective and comprehensive the AML controls, the lower the final vulnerability of the product.

Figure 11.a: Output charts (applicable in case of product-based assessment, Excel File 6.B)

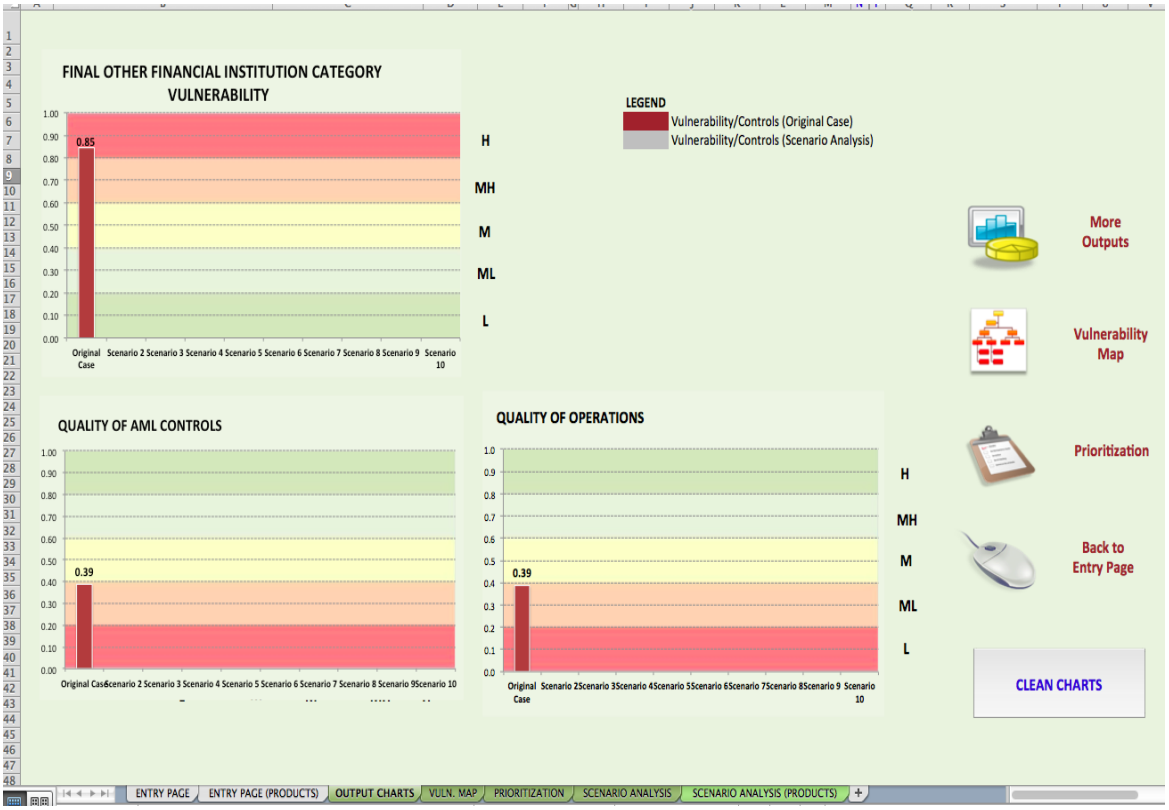
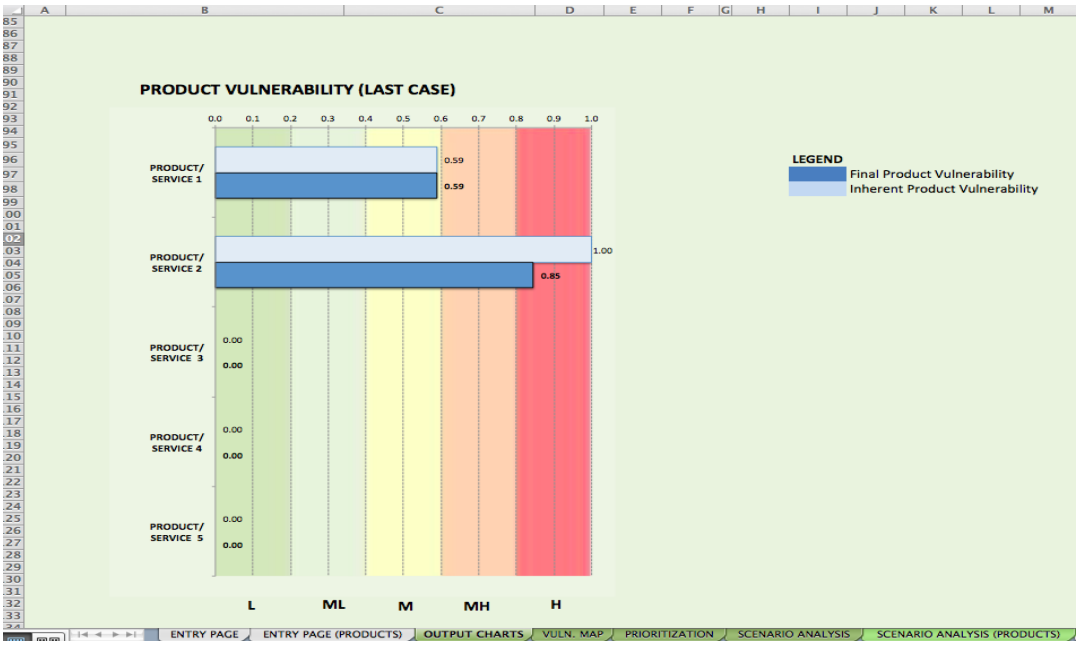


Figure 11.b: Product Vulnerability Output (only in product-based assessment, Module 6.B)



For both the product vulnerability chart and the final vulnerability of the assessed Other FI category chart, a higher score implies a higher vulnerability to ML. Similarly; a higher product vulnerability score increases the vulnerability score of the assessed Other FI category.

On the other hand, for intermediate variables that relate to controls (such as *Quality of AML Controls, Quality of CDD Framework*, and *Quality of Operations*) a higher score indicates a higher combating ability, which lowers the vulnerability of the assessed Other FI category to ML.

Applicable to both Excel files (6.A and 6.B)

For vulnerability-related charts, a lower score is indicated by shades of green, implying lower ML vulnerability. On the other hand, for intermediate variables related to AML controls, a lower score is indicated by shades of red, implying a lower combating ability, and hence higher ML vulnerability.

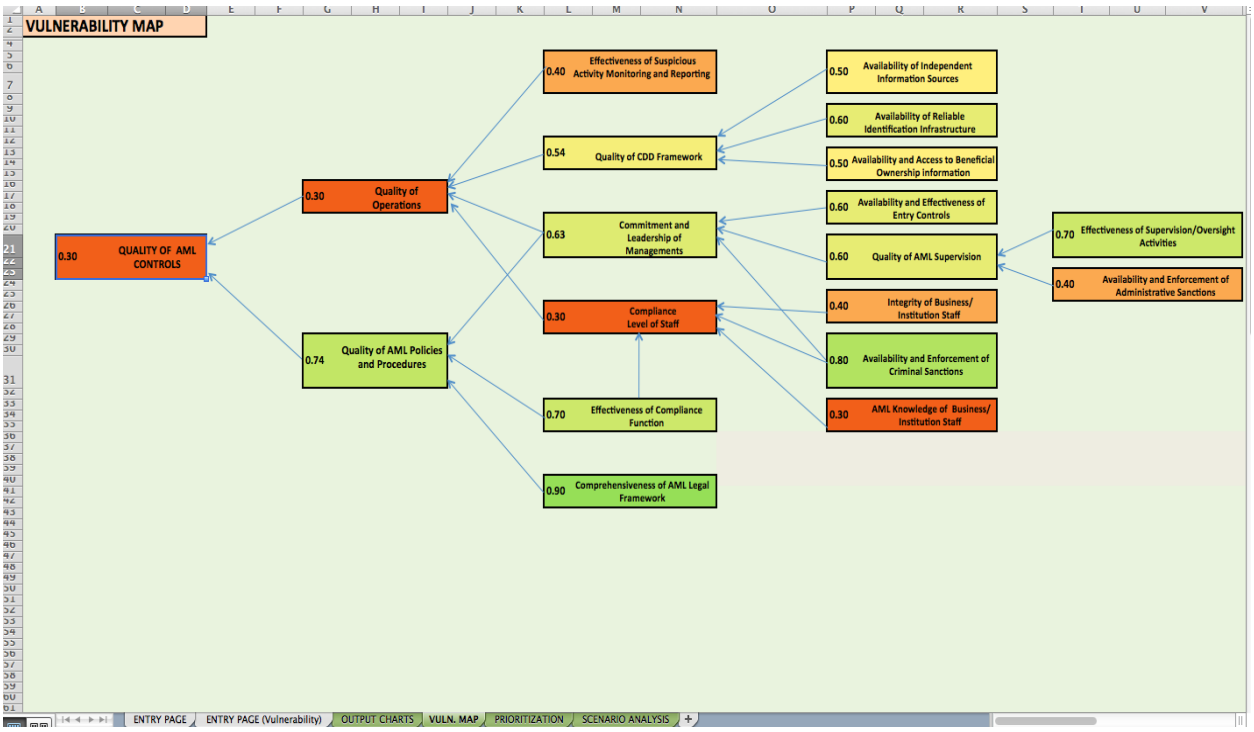
Please pay attention to the names and the colors of the inputs and outputs while interpreting the scores.

- When the reference is to "vulnerability," a low score is desired; therefore low corresponds to green and high corresponds to red.
- When the reference is to "controls" or related inputs, a high score, which means better controls, is desired. Therefore, for control related inputs and outputs, high corresponds to green and low corresponds to red.

(2) Vulnerability Map tab

Vulnerability Map is a visual summary of the assessment, which shows how the assessment inputs cause impact on the outputs. To view the vulnerability map of the assessed Other FI category, click on the **Vulnerability Map** icon on the Entry Page (Vulnerability) tab (as shown in Figure 8) or Entry Page (Products) tab (as shown in Figure 9) for product based assessment- Excel file 6.B. This tab provides a visual summary of the assessment ratings of all the variables (see Figure 12). Note that the vulnerability map only shows the network diagram for the assigned assessment ratings of general input variables, and the corresponding assessment results of the intermediate variables, which affect the degree to which the assessed Other FI category is able to combat ML. This diagram does not show the effect of general input variables on product vulnerability, or the impact of product vulnerabilities on the final vulnerability of the assessed Other FI category (applicable only in case of product based assessment- Excel file 6.B).

Figure 12: Vulnerability Map (applicable to both Excel files, 6.A and 6.B)

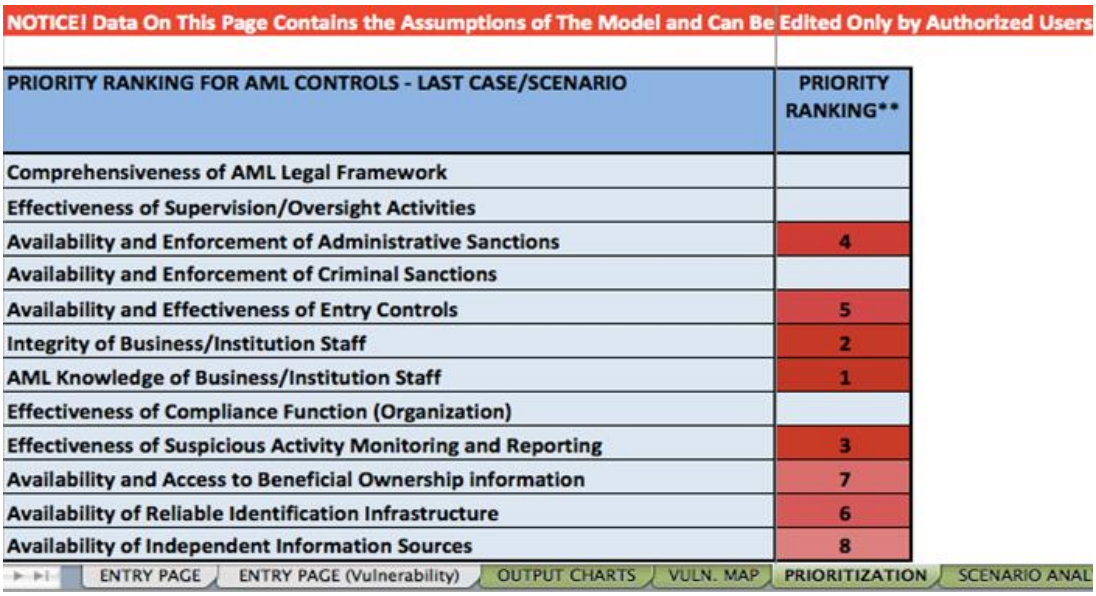


The assessment results in Figure 12 show that the quality of AML controls is weak. This can be seen in the low score and the red color of the box, both of which indicate weak AML controls. Although the *Quality of AML Policies and Procedures* is good (this type of green indicates a medium-high score), the *Quality of Operations in* Other FI category is weak (the low score and the color red indicating weak operations). The problem area is therefore *Quality of Operations*. Low *Compliance Level of Staff* and weak *Suspicious Activity Monitoring and Reporting Systems* in the Other FI category underlie the deficiencies in operations. Furthermore, low *Integrity of Business/Institution Staff* and low *AML Knowledge of Business/Institution Staff* are the factors underlying Low *Compliance Level of Staff in* Other FI category.

(3) Prioritization tab

A priority ranking can be generated to help guide relevant authorities to prioritize actions to strengthen AML controls within the assessed Other FI category. Click on the **Prioritization** icon in the Entry Page (Vulnerability) tab (Figure 8) or in the Output Charts tab (Figure 10) to go to the Prioritization tab. In case of product based assessment (Excel file 6.B), Click on the **Prioritization** icon in the Entry Page (Products) tab (Figure 9) or in the Output Charts tab (Figure 11.a) to go to the Prioritization tab. The table in the Prioritization tab ranks the general input variables with respect to their impact on the AML controls and consequently the vulnerability of the assessed Other FI category (see Figure 13).

Figure 13: Prioritization table (applicable to both the Excel files, 6.A and 6.B)



NOTICE! Data On This Page Contains the Assumptions of The Model and Can Be Edited Only by Authorized Users

PRIORITY RANKING FOR AML CONTROLS - LAST CASE/SCENARIO	PRIORITY RANKING**
Comprehensiveness of AML Legal Framework	
Effectiveness of Supervision/Oversight Activities	
Availability and Enforcement of Administrative Sanctions	4
Availability and Enforcement of Criminal Sanctions	
Availability and Effectiveness of Entry Controls	5
Integrity of Business/Institution Staff	2
AML Knowledge of Business/Institution Staff	1
Effectiveness of Compliance Function (Organization)	
Effectiveness of Suspicious Activity Monitoring and Reporting	3
Availability and Access to Beneficial Ownership information	7
Availability of Reliable Identification Infrastructure	6
Availability of Independent Information Sources	8

- A low number, highlighted in a darker color/dark red, signifies that the general input variable merits a high priority in the action plan.
- A high number, highlighted in a lighter red (or pink), means that corresponding input variable still has severe deficiencies and is in the priority list, although it has less priority than the ones with darker colors.
- A blank cell (in light blue) indicates that the corresponding input variable does not have priority. There may still be deficiencies related to variable, but these are not severe and do not require urgent action.

For example, in Figure 13, the input variable *AML Knowledge of Business/Institution Staff* has a priority ranking of one, implying that mitigating the deficiency related to this variable is the first item at the top of the priority list. The prioritization table results should be used as a starting point for developing action plans.

Please note that the variable that has the lowest rating in the Entry Page tab may not have the highest priority rating in most cases. Priority rankings do not necessarily run parallel with the ratings in the Entry Page tab. Sometimes an item that is rated as medium may turn out to have the highest priority. Such

results are fully consistent with the logic of the tool; as the assessment rating is just one of the four factors that have an impact on priority ranking. As previously explained, the other three factors are:

1. The network structure of the module
2. The weights of the input and intermediate variables
3. The defined conditions (prerequisites) for intermediate variables.

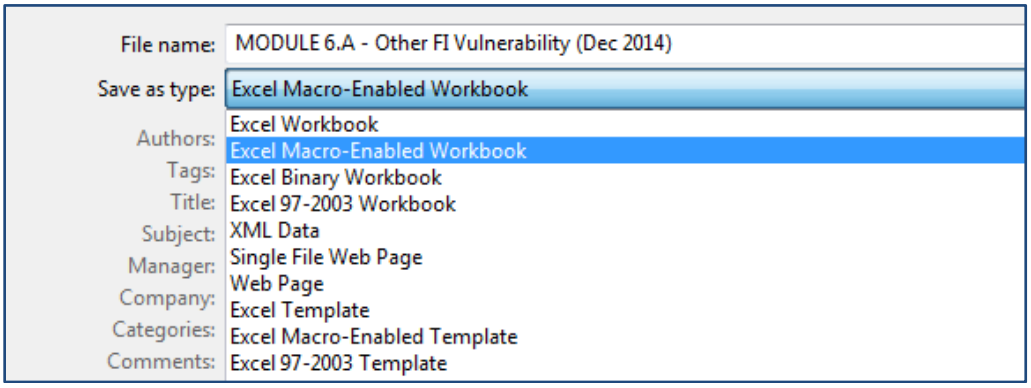
Applicable to product-based assessment (Excel File 6.B)

Whether an Open Door Approach or a Weighted Average Approach (or a combination of both approaches) is used to assess the vulnerability of the Other FI category, all the outputs and assessment results discussed in Step 5 will be the same for all three approaches. Only the final vulnerability of the assessed Other FI category will vary for the three different approaches.

Step 6: Saving the file

Save the file. It is important to save the file as a macro-enabled workbook (as shown in Figure 14). If it is not saved as a macro-enabled workbook, the macros will be disabled and the Excel file will not function properly.

Figure 14: Save Excel file as a macro-enabled workbook (applicable to both the Excel files)



Changing entries after the original case has been saved

If any changes have been made to the original case entries, remember to save those entries by clicking on the **Save the Original Case** icon on the Entry Page (Vulnerability) tab (see Figure 8) or Entry Page (Products) tab (see Figure 9) in case of product based assessment- Excel file 6.B. The assessment outputs will not reflect the changes unless the entries have been saved.

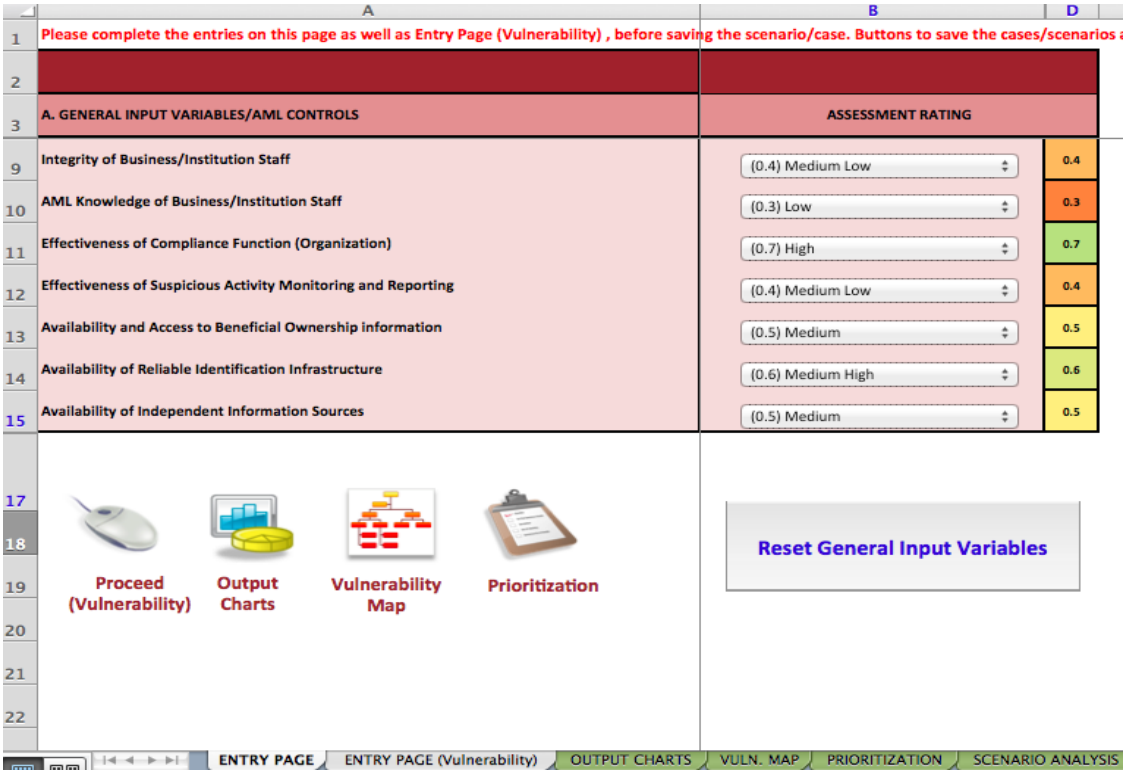
Erase all the entries and restart the process
Click the **Reset Inherent Vulnerability Entries** icon on the Entry Page (Vulnerability) tab (Figure 8), and click the **Reset General Input Variables** icon on the Entry Page tab (Figure 15) to erase all the previous entries. Also click the **Clean Charts** icon on the Output Charts tab (Figure 10) to erase the previous entries on the Output Charts tab.

Applicable to product-based assessment (Excel File 6.B)

Click the **Reset Product Entries** icon on the Entry Page (Products) tab (Figure 9), and click the **Reset General Input Variables** icon on the Entry Page tab (Figure 15) to erase all the previous entries. Also click

the **Clean Charts** icon on the Output Charts tab (Figure 11.a) to erase the previous entries on the Output Charts tab.

Figure 15: Icons on the Entry Page tab (applicable to both the Excel files, 6.A and 6.B)



Step 7: Using the Excel file for scenario analysis (optional)

The Excel file can also be used for scenario analysis. It can be used either for comparing the vulnerability of the assessed Other FI category over a period of time, or for observing and analyzing the effects of various policy options, based on scenarios. For example, it is possible to see what impact policy actions (individually or collectively) may have on reducing vulnerability.

Similarly, the assessment ratings for general input variables, final and inherent vulnerability of the assessed Other FI category, assessment results for intermediate variables, and priority ranking for the general input variables for different years or scenarios can all be compared using the scenario analysis option.

In case of product based assessment (Excel file 6.B), it can also be used for comparing the final and inherent vulnerabilities of the products for different years or scenarios. It is also possible to use the scenario analysis function for comparing the results of Open Door and Weighted Average Approaches.

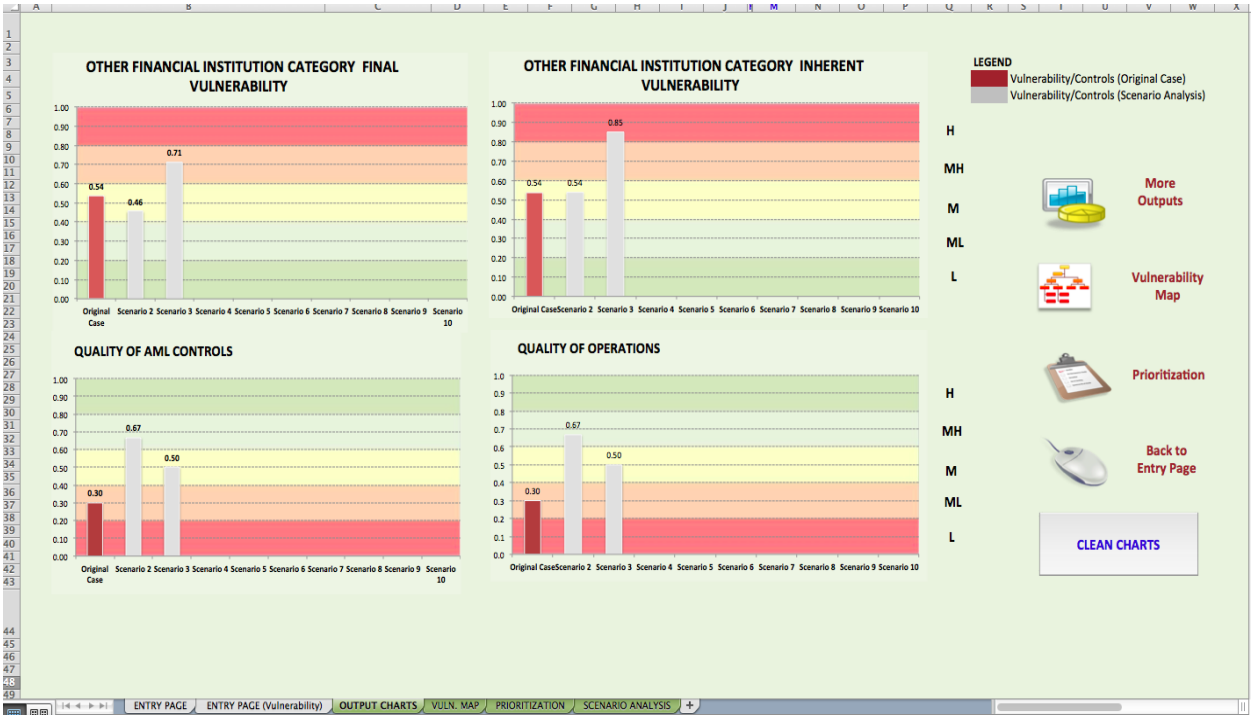
Instructions for using the scenario analysis option (Excel File 6.A)

To use the scenario analysis option, first be sure to save the Excel file with the original entries, and then create a new copy of the file for scenario analysis. Then go to the Entry Page tab, and make sure you do

not reset the entries. Insert the new assessment ratings for the general input variables and inherent vulnerability variables for the second year, or for scenario 2, in the Entry Page tab and Entry Page (Vulnerability) tab respectively and save the entries as Scenario 2 (as shown in Figure 8).

As in Step 5, assessment results are generated in the Output Charts tab (as shown in Figure 16). Note that in a scenario analysis, the original case results are shown in brown while all scenario 2/second year results are shown in gray (see Figure 16). Scenario analysis can be performed for 10 years, or for 10 different scenarios. The assessment results for the final and inherent vulnerability of the assessed Other FI category and the intermediate variables (such as *Quality of AML Controls* and *Quality of Operations*) are available for all the years (as shown in Figure 16).

Figure 16: Output charts – Scenario Analysis (Excel File 6.A)



***Instructions for using the scenario analysis option for* product-based assessment (Excel File 6.B)**

To use the scenario analysis option, first be sure to save the Excel file with the original entries, and then create a new copy of the file for scenario analysis. Then go to the Entry Page tab, and make sure you do not reset the entries. Insert the new assessment ratings for the general input variables and product specific input variables for the second year, or for scenario 2, in the Entry Page tab and Entry Page (Products) tab respectively and save the entries as Scenario 2 (as shown in Figure 9).

As in Step 5, assessment results are generated in the Output Charts tab (as shown in Figure 17.a and Figure 17.b). Note that in a scenario analysis, the original case results are shown in brown while all scenario 2/second year results are shown in gray (see Figure 17.a). Scenario analysis can be performed for 10 years, or for 10 different scenarios. In Figure 17.b, the vulnerability assessment results of the products are produced only for the last case (i.e., the third year/Scenario 3). The assessment results for the vulnerability

of the assessed Other FI category and the intermediate variables (such as *Quality of AML Controls* and *Quality of Operations*) are available for all the previous cases, as well as the last case (as shown in Figure 17.a).

Figure 17.a: Output charts – Scenario Analysis (Excel File 6.B)

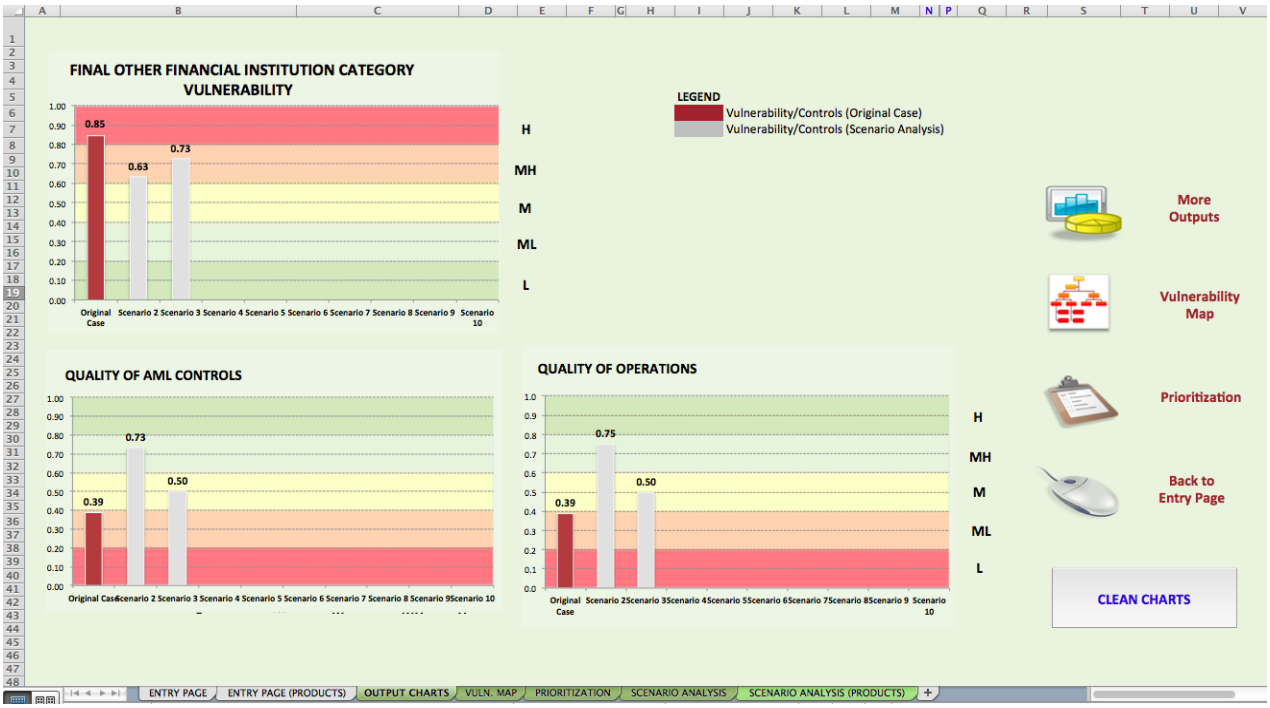
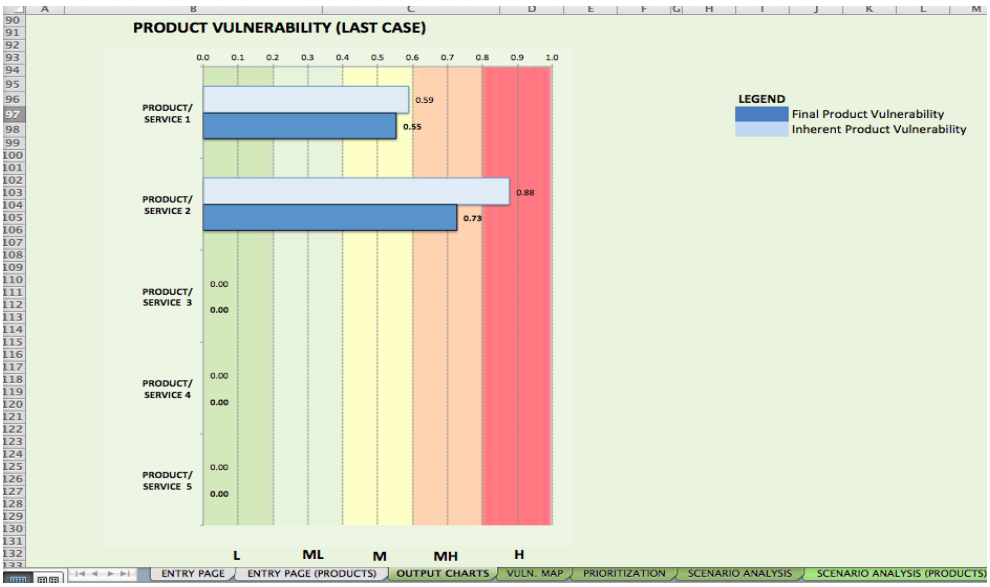


Figure 17.b: Product Vulnerability Output chart– Scenario Analysis (Excel File 6.B)



Scenario Analysis results - screen display (Excel Files 6.A and 6.B)

The Scenario Analysis tab provides the assessment results for the different years or scenarios (Figure 18). The Scenario Analysis tab shows the assigned assessment ratings for the general input variables, the

assessment results for intermediate variables, the final and inherent vulnerability of the assessed Other FI category, and the priority rankings of the general input variables for the various years/scenarios. These tables are helpful in understanding where changes in the vulnerability of the assessed Other FI category originate, as well as the impact of policy actions on vulnerability, the combating ability/AML controls and the priority ranking of general input variables. The tables show how policy actions have an impact on the various components of vulnerability over a period of time, or in different scenarios.

Figure 18: Scenario Analysis tab (Excel Files 6.A and 6.B)

	Original Case	Scenario 2	Scenario 3	Sc
INPUTS - GENERAL INPUT VARIABLES/AML CONTROLS				
Comprehensiveness of AML Legal Framework	0.9	0.9	0.5	
Effectiveness of Supervision/Oversight Activities	0.7	0.7	0.5	
Availability and Enforcement of Administrative Sanctions	0.4	0.6	0.5	
Availability and Enforcement of Criminal Sanctions	0.8	0.8	0.5	
Availability and Effectiveness of Entry Controls	0.6	0.6	0.5	
Integrity of Business/Institution Staff	0.4	0.6	0.5	
AML Knowledge of Business/Institution Staff	0.3	0.7	0.5	
Effectiveness of Compliance Function (Organization)	0.7	0.7	0.5	
Effectiveness of Suspicious Activity Monitoring and Reporting	0.4	0.8	0.5	
Availability and Access to Beneficial Ownership information	0.5	0.5	0.5	
Availability of Reliable Identification Infrastructure	0.6	0.6	0.5	
Availability of Independent Information Sources	0.5	0.8	0.5	
OUTPUTS/ASSESSMENT RESULTS FOR INTERMEDIATE VARIABLES				
OTHER FINANCIAL INSTITUTION CATEGORY FINAL VULNERABILITY	0.54	0.46	0.71	
OTHER FINANCIAL INSTITUTION CATEGORY INHERENT VULNERABILITY	0.54	0.54	0.85	
QUALITY OF AML CONTROLS	0.30	0.67	0.50	
Quality of Operations	0.30	0.67	0.50	
Quality of AML Policies and Procedures	0.74	0.76	0.50	
Quality of CDD Framework	0.54	0.59	0.50	
Compliance Level of Staff	0.30	0.69	0.50	
Quality of AML Supervision	0.60	0.67	0.50	
Commitment and Leadership of Managements	0.63	0.67	0.50	
PRIORITY RANKING FOR GENERAL INPUT VARIABLES/AML CONTROLS				
Comprehensiveness of AML Legal Framework			3	
Effectiveness of Supervision/Oversight Activities			2	
Availability and Enforcement of Administrative Sanctions	4	3	8	
Availability and Enforcement of Criminal Sanctions			9	
Availability and Effectiveness of Entry Controls	5	1	5	
Integrity of Business/Institution Staff	2	2	6	
AML Knowledge of Business/Institution Staff	1		1	
Effectiveness of Compliance Function (Organization)			3	
Effectiveness of Suspicious Activity Monitoring and Reporting	3		7	
Availability and Access to Beneficial Ownership information	7	5	11	
Availability of Reliable Identification Infrastructure	6	4	10	
Availability of Independent Information Sources	8		12	

ENTRY PAGE | ENTRY PAGE (Vulnerability) | OUTPUT CHARTS | VULN. MAP | PRIORITIZATION | SCENARIO ANALYSIS

Scenario Analysis results - screen display for product-based assessment (Excel File 6.B)

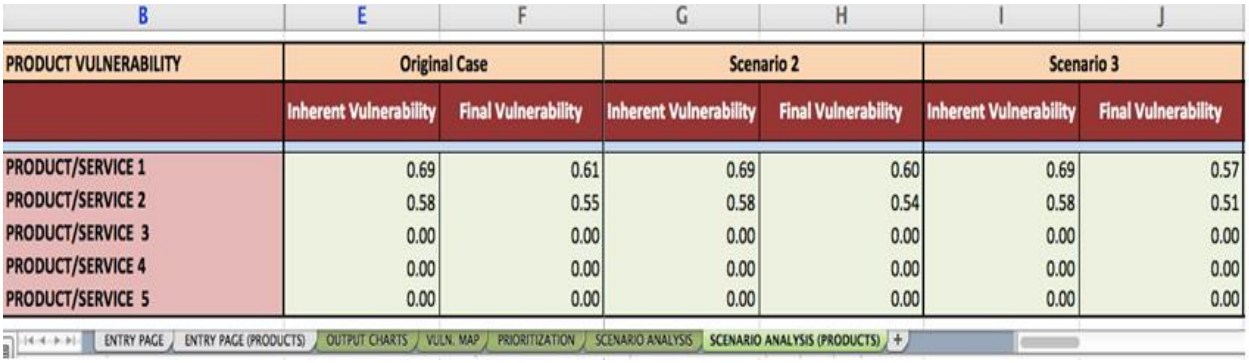
The Scenario Analysis and Scenario Analysis (Products) tabs provide the assessment results for the different years or scenarios. The Scenario Analysis tab shows the assigned assessment ratings for the

general input variables, the assessment results for intermediate variables, the final vulnerability of the assessed Other FI category, and the priority rankings of the general input variables for the various years/scenarios (Figure 18).

The Scenario Analysis (Products) tab shows the inherent and final vulnerability for the products assessed for the various years/scenarios (Figure 19).

These tables are helpful in understanding where changes in the vulnerability of the assessed Other FI category originate, as well as the impact of policy actions on vulnerability, the combating ability/AML controls, the product vulnerability, and the priority ranking of general input variables. The tables show how policy actions have an impact on the various components of vulnerability over a period of time, or in different scenarios.

Figure 19: Scenario Analysis (Products) tab (Excel File 6.B)



B	E	F	G	H	I	J
PRODUCT VULNERABILITY	Original Case		Scenario 2		Scenario 3	
	Inherent Vulnerability	Final Vulnerability	Inherent Vulnerability	Final Vulnerability	Inherent Vulnerability	Final Vulnerability
PRODUCT/SERVICE 1	0.69	0.61	0.69	0.60	0.69	0.57
PRODUCT/SERVICE 2	0.58	0.55	0.58	0.54	0.58	0.51
PRODUCT/SERVICE 3	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE 4	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE 5	0.00	0.00	0.00	0.00	0.00	0.00

ENTRY PAGE | ENTRY PAGE (PRODUCTS) | OUTPUT CHARTS | VULN. MAP | PRIORITIZATION | SCENARIO ANALYSIS | SCENARIO ANALYSIS (PRODUCTS) | +

How to "unhide" the Weights tab

The default weights of the variables and prerequisites of the intermediate variables reflect the assumptions that underlie the module. In the default version of the Excel file, the weights, the defined prerequisites cannot be changed by users, but can be viewed. These weights can be revealed by clicking on the **Weights tab**. To reveal the weights tab, select any tab, right click on the name of the tab, and click the **Unhide** option. When the Unhide window opens, click on the **Weights** option and press **OK**. Note that the Weights tab is protected and no changes can be made to this sheet. Contact the World Bank NRA Team if changes to the weights and prerequisites are required.

In Figure 20, column B shows the weights for the variables in the Excel file. The weights assigned to the variables are relative. For example, the variable *Quality of Operations (line 5)* is determined by four variables:

- *Quality of CDD Framework (line 6)*
- *Effectiveness of Suspicious Activity Monitoring and Reporting (line 10)*
- *Compliance Level of Staff (line 11)*
- *Commitment and Leadership of Managements (line 19).*

Figure 20: Weights tab (applicable to both Excel files, 6.A and 6.B)

	A	B	C
1	NOTICE! Data on this page contains the assumptions of the model and can be edited only by Authorized Users		
2	VULNERABILITY OF THE OTHER FINANCIAL INSTITUTION CATEGORY	WEIGHTS	PREREQUISITES
3	1. AML CONTROLS FOR THE OTHER FINANCIAL INSTITUTION CATEGORY (Quality of AML Controls)	2	0
5	1.1. Quality of Operations	1	1
6	1.1.1. Quality of CDD Framework	1	0
7	1.1.1.1. Availability of Reliable Identification Infrastructure	3	1
8	1.1.1.2. Availability and Access to Beneficial Ownership information	3	0
9	1.1.1.3. Availability of Independent Information Sources	1	0
10	1.1.2. Effectiveness of Suspicious Activity Monitoring and Reporting	2	0
11	1.1.3. Compliance Level of Staff	3	1
12	1.1.3.1. Integrity of Business/Institution Staff	2	0
13	1.1.3.2. AML Knowledge of Business/Institution Staff	3	1
14	1.1.3.3. Effectiveness of Compliance Function	2	0
18	1.1.3.4. Availability and Enforcement of Criminal Sanctions	1	0
19	1.1.4. Commitment and Leadership of Managements	3	1
20	1.1.4.1. Availability and Effectiveness of Entry Controls	2	0
21	1.1.4.2 Quality of AML Supervision	4	0
22	1.1.4.2.1 Effectiveness of Supervision/Oversight Activities	2	1
23	1.1.4.2.2 Availability and Enforcement of Administrative Sanctions	1	0
24	1.1.4.3. Availability and Enforcement of Criminal Sanctions	1	0
25	1.2. Quality of AML Policies and Procedures	1	1
26	1.1.2.1. Comprehensiveness of AML Legal Framework	1	0
27	1.1.2.2. Commitment and Leadership of Managements	1	0
28	1.1.2.3. Effectiveness of Compliance Function	1	0
33	2. INHERENT VULNERABILITY OF THE OTHER FINANCIAL INSTITUTION CATEGORY	3	1
34	2.1. Total Size/Volume	3	
36	2.2. Client Base Profile	3	
37	2.3. Use of Agents	3	
38	2.4. Level of Cash Activity	2	
41	2.5. Frequency of International Transactions	3	
42	2.6. Other Vulnerable Factors	3	
50			

ENTRY PAGE | ENTRY PAGE (Vulnerability) | WEIGHTS | OUTPUT CHARTS | VULN. MAP | PRIORITIZATION | SCENARIO ANALYSIS | +

The weights on these four variables in determining the *Quality of Operations* (line 5) are relative to one another, as follows. The weight of the variable *Compliance Level of Staff (line 11)* is three times that of the variable *Quality of CDD Framework (line 6),* while the variable *Quality of AML Controls* (line 3) is determined equally by the variables *Quality of Operations* (line 5) and *Quality of AML Policies and Procedures (line 25)* (both have an assigned weight of 1).

The defined prerequisites for the intermediate variables are shown in column C (see Figure 21). If a variable has a weight of 1 assigned to it in column C, then it is a prerequisite. For example, for the variable *Quality of CDD Framework (line 6)*, the variable *Availability of Reliable Identification Infrastructure (line 7)* is a prerequisite. This means that the variable *Quality of CDD Framework* cannot be better than the variable *Availability of Reliable Identification Infrastructure.* In other words, the score of the lower-level variable defines a cap on the score of the higher- level variable.

ANNEX 2 - PRODUCT-BASED ASSESSMENT MODULE (MODULE 6.B)

The Working Group can decide to undertake a more detailed assessment of the products being offered by the assessed Other FI category. This is to be decided on a needs basis as discussed in section 2.1.

Assess different products in the Other FI category only if the products have different money laundering risks and there are benefits to be derived from detailed separate product analysis.

Why perform an assessment of certain products?

Certain products are inherently more vulnerable to money laundering. This increased vulnerability may arise from the characteristics of the product- such as the availability of anonymous use, non-face-to-face interactions, frequent use of cash- or the characteristics of the clients such as PEPs or high wealth individuals who are likely to make use of the product. Since, the inherent factors may differ among the products, we need to assess the inherent vulnerability of each product separately.

Module Structure (The Network)

As illustrated in Figure 21, the overall vulnerability of the Other FI category is determined by the vulnerabilities of the various products assessed for the other FI category. This module assumes that product vulnerability can be measured by two main factors*, which are determined by underlying sub-factors*: *1-Inherent Vulnerability (of the product) and 2-Quality of AML Controls.* "Product 1" is used as an example in Figure 21. Similar assessments can be performed for Other FI categories, and up to 5 products for each Other FI category.

Guidance for Assessment of Variables

For the assessment of AML control variables, refer to Section 4.1, where you can find assessment worksheets for AML control variables. The criteria for assessing AML controls variables in product-based module are the same as the criteria for assessing the AML controls variables for the specific Other FI category. Similarly, the criteria for assessing inherent vulnerability variables for each product are the same as the criteria for assessing broader inherent vulnerability factors for the specific Other FI category. For assessment worksheets on inherent vulnerability variables, refer to Section 4.2.

Figure 21: Product-based Other FI Vulnerability Module Structure (Excel File 6.B)