WORLD BANK GROUP
Finance & Markets

NRA toolkit

NATIONAL RISK ASSESSMENT TOOL
GUIDANCE MANUAL

MODULE 3
BANKING SECTOR VULNERABILITY

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 development of Banking Sector Vulnerability Module of the National ML/TF Risk Assessment Tool was initiated and led by Emiko Todoroki. Together with Ms. Todoroki, Louis de Koker, and Massoud Moussavi developed the original concept that was based on a Bayesian Network. Kuntay Celik has developed the Excel based version of the model and supported the team in developing the assessment templates. 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 the 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 assessment and will limit the benefits the jurisdiction can derive from the assessment.
- During the assessment, please clearly identify any problems, weaknesses, or gaps by determining what is missing and what is not working. Such an approach will help you draw up the 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 National Risk Assessment report.

1. OBJECTIVES OF THE BANKING SECTOR VULNERABILITY MODULE

The main objectives of Banking Sector Vulnerability Module (the module) are to:

- Identify the overall vulnerability of the banking sector
- Identify bank products/services/channels[1] with high vulnerability
- Prioritize action plans that will strengthen anti-money laundering controls (AML controls) in the banking sector.

The outcome of Banking Sector Vulnerability Assessment is necessary for:

- Designing action plans for more effective AML policies and practices throughout the sector
- Evaluating the impact of different interventions by regulatory (and other relevant) authorities
- Comparing the level of vulnerability in the banking sector with the vulnerability in other financial sectors
- Ensuring efficient resource allocation
- Developing specific AML controls for high-risk products.

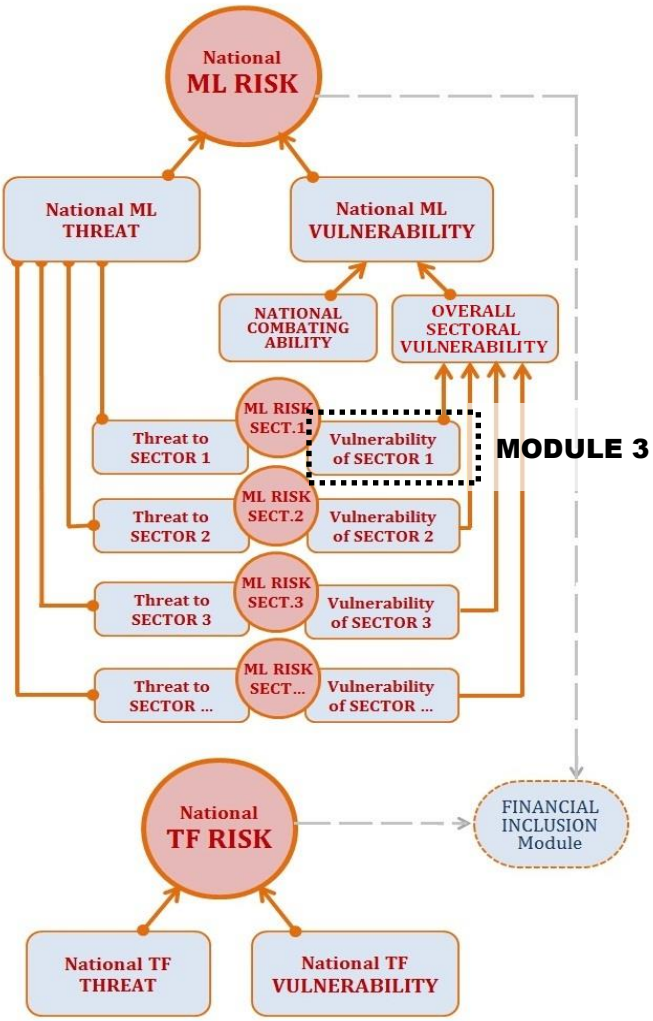
[1] The assessment may include products (e.g., deposit accounts), services (e.g., asset management), or channels (e.g., electronic banking). For simplicity, this document will subsequently refer only to products. This reference should be understood as products, services, or channels.

2. UNDERSTANDING THE BANKING SECTOR VULNERABILITY MODULE

2.1. Banking Sector 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 banking sector's vulnerability to money laundering and the money laundering threat to banking sector together cause the money laundering risk to the banking sector. In addition to the risk at sector level, the vulnerability of the banking sector has an impact on the national vulnerability.

Figure 1: Banking Sector 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 any 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 banking sector.

2.2. 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 variable in the module: (1) input variables, and (2) intermediate variables.

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

    a. ***AML control variables*** are also broken down into two subtypes: General AML controls, and Product-specific AML controls:

        i. *General AML controls.* These apply to the entire banking sector, and should be assessed at sector level. This type of input variables relate to the quality and effectiveness of general AML controls, and therefore affects the vulnerability of all the products being assessed.

        ii. *Product-specific AML controls.* These controls are designed specifically for a particular product. They therefore only impact the vulnerability of the product they are related to.

    b. ***Inherent vulnerability variables*** relate to specific features and users of a particular product. An example would be a client base profile. As the client base profile may vary from product to product, and consequently affect its vulnerability, it is necessary to assess to client profiles separately for different products.

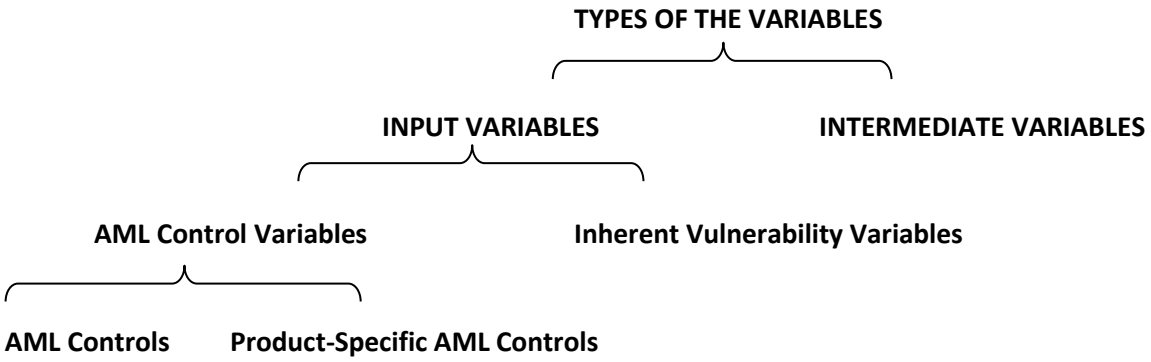
2. **Intermediate variables** are broad and high-level factors that cannot be assessed directly. They therefore need to be disaggregated into their constituent parts in order to be assessed. The module determines intermediate variables automatically, based on the ratings entered for the input variable. 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 input variables and intermediate variables in more detail. Descriptions of the intermediate variables can be found in Section 5 of this document.

General AML control variables relate to the effectiveness of the general AML controls, and are relevant for all banking sector products. This is because banking sectors that are well supervised for AML purposes by well-trained and committed officials have reduced vulnerability on all offered products.

Other input variables relate to inherent vulnerability factors that are specific to a particular product: e.g., the total value of that product, the level of cash activity, its client base profile, or the channel through which it is offered. These input variables are called inherent vulnerability variables.

In addition, a third type of input variable – a specific control variable – exists for each product. Although this variable is not an inherent vulnerability variable, it is product-specific, and needs to be assessed for each product separately. This input variable is called product-specific AML control variable. Figure 2 provides a visual summary of the various types of variables.

Figure 2: Variables in the Banking Sector Vulnerability Module



The relationship between this breakdown and the module structure in Figure 3.a is as follows (see colored boxes in Figure 3.a):

- Intermediate variables (pink boxes) do not require assessment.
- General AML control variables (green boxes) need to be assessed for entire sector.
- Inherent vulnerability variables (blue boxes) need to be assessed for each product.
- Product-specific AML controls[2] (blue box with green borders) needs to be assessed for each product.

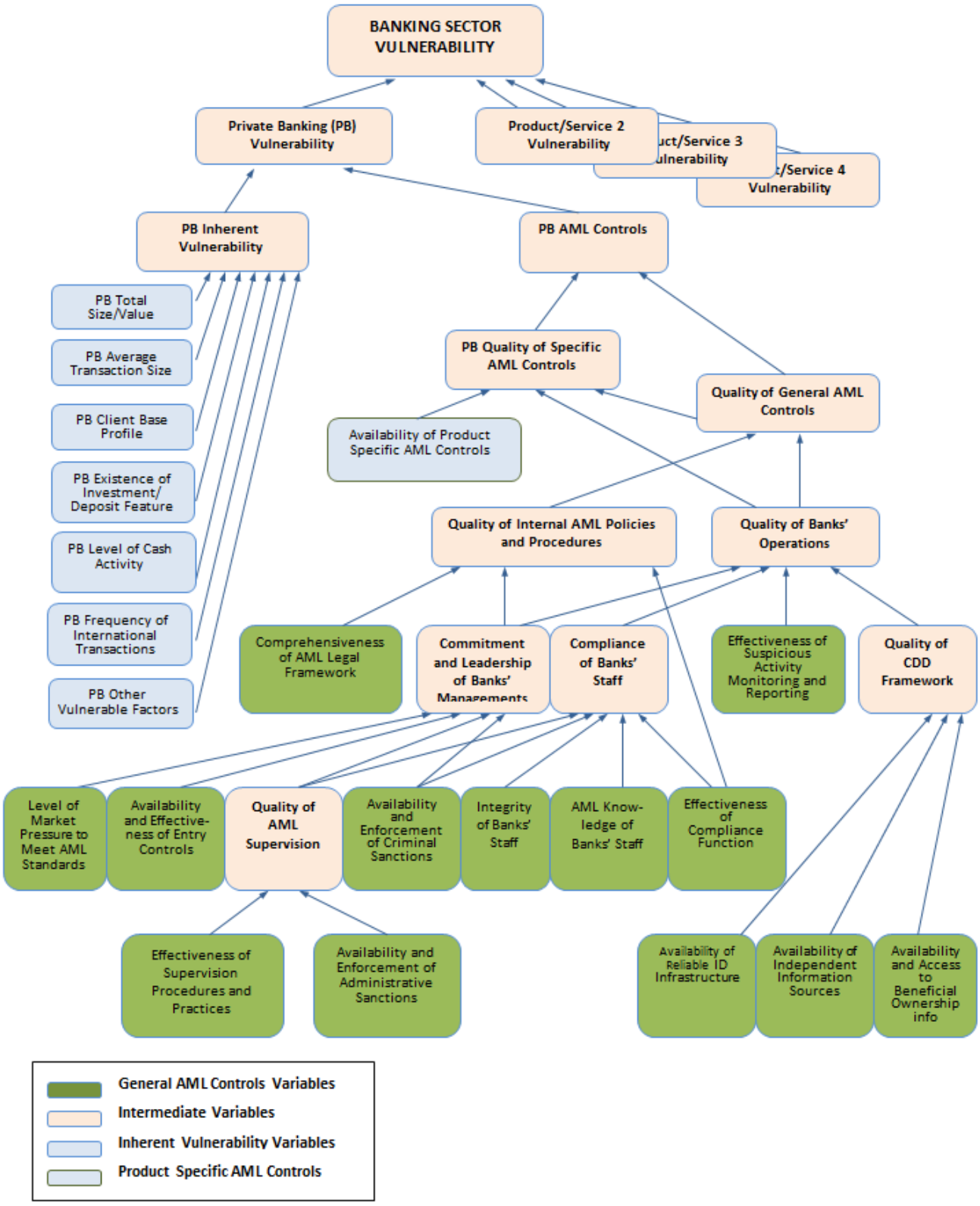
2.3. Module Structure (The Network)

The module is based on the assumption that the sector is similar to a building, with the products on offer being the various entrances to the building. Any money -laundering attempt needs to enter the banking sector through one of these doors. Therefore, assessing the vulnerabilities of all the doors provides a measure of the overall vulnerability of the building against any unauthorized entry. Similarly, the module assumes that assessing the vulnerabilities of all the products offered by the sector will lead us to the overall vulnerability of the sector.

As illustrated in Figure 3.a, the overall vulnerability of the banking sector is determined by the vulnerabilities of its various products. Assessing the vulnerability of existing products therefore contributes to a comprehensive assessment of the vulnerability of the banking sector as a whole. 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) AML controls (for the product). An example, used in Figure 3.a, is private banking. Similar assessments can be performed for twenty products.

Figure 3.a: Banking Sector Vulnerability Module structure

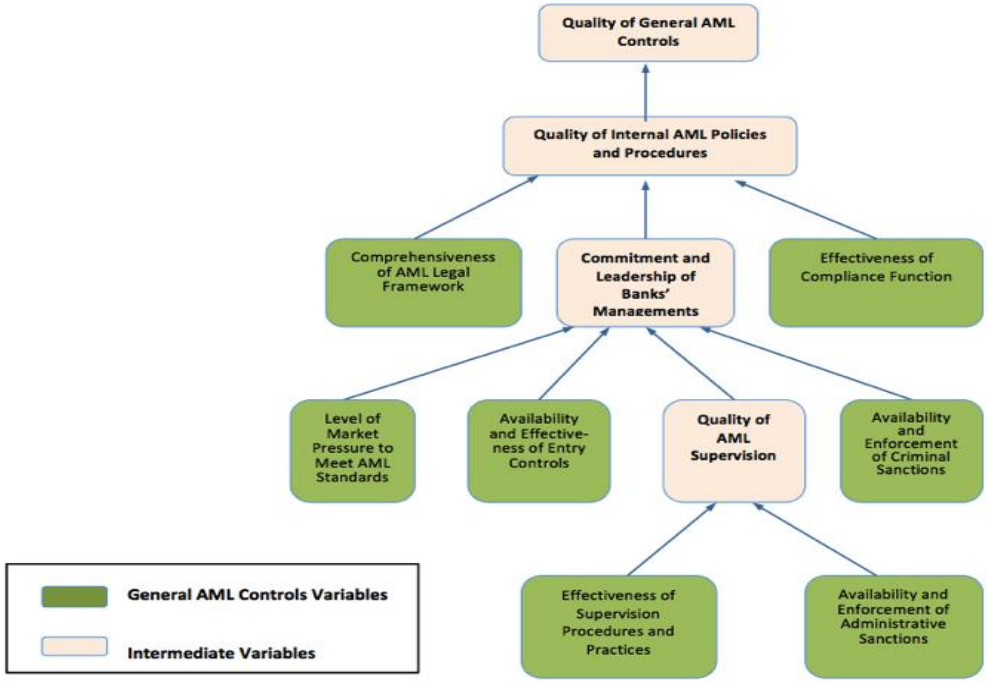
[2] The colors used for the *Specific AML Controls* represent its similarities with other variables. It is filled in blue, since it needs to be assessed separately for each product (cf. inherent vulnerability variables). Its borders are green, to show that it is a part of AML controls.


BANKING SECTOR VULNERABILITY
Private Banking (PB) Vulnerability
Product/Service 2 Vulnerability
Vulnerability
Vulnerability
PB Inherent Vulnerability
PB AML Controls
PB Total Size/Value
PB Average Transaction Size
PB Client Base Profile
PB Existence of Investment/ Deposit Feature
PB Level of Cash Activity
PB Frequency of International Transactions
PB Other Vulnerable Factors
PB Quality of Specific AML Controls
Quality of General AML Controls
Availability of Product Specific AML Controls
Quality of Internal AML Policies and Procedures
Quality of Banks' Operations
Comprehensiveness of AML Legal Framework
Commitment and Leadership of Banks' Managements
Compliance of Banks' Staff
Effectiveness of Suspicious Activity Monitoring and Reporting
Quality of CDD Framework
Level of Market Pressure to Meet AML Standards
Availability and Effective-ness of Entry Controls
Quality of AML Supervision
Availability and Enforcement of Criminal Sanctions
Integrity of Banks' Staff
AML Know-ledge of Banks' Staff
Effectiveness of Compliance Function
Effectiveness of Supervision Procedures and Practices
Availability and Enforcement of Administrative Sanctions
Availability of Reliable ID Infrastructure
Availability of Independent Information Sources
Availability and Access to Beneficial Ownership info
General AML Controls Variables
Intermediate Variables
Inherent Vulnerability Variables
Product Specific AML Controls

2.3 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 the **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 banking sector affects the quality of general 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 banks' managements. This supervisory pressure strengthens the commitment of banks' managements to ensure AML compliance and to show leadership in the matter. As a result, managements start to take action to improve the quality of their internal AML policies and procedures. Eventually, the banks begin to have better general AML controls. As a result, the vulnerabilities of various products, as well as the banks overall vulnerability 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 the second input variable, *Effectiveness of Supervision Procedures and Practices*. Assessing this second variable together with *Availability and Enforcement of Administrative Sanctions* will provide a good assessment of the *Quality of AML Supervision*. Note that the *Availability and Enforcement of*

Administrative Sanctions and *Effectiveness of Supervision Procedures and Practices* are both input variables to *Quality of AML Supervision*, which is an intermediate variable. Input variables require direct input from the WG, while 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, please see Section 5.

Factors that determine the vulnerability of the banking sector

There are four factors that determine banking sector vulnerability. These are:

- The network structure of the module
- The relative weights of the input variables and the intermediate variables
- The defined conditions (prerequisites) for intermediate variables
  The assessment ratings for the input variables.

The assessment ratings for 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 a weighted linking of the underlying relationships of input variables. These formulas can be viewed (i.e., "unhidden") – see the Annex for further information. Changes to these formulas can only be made by the World Bank. Please contact the World Bank NRA Team for further information, if changes are required.

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 sector vulnerability in various directions.

- **General AML controls.** Higher ratings reduce the banking sector vulnerability; lower ratings increase the banking sector vulnerability.

- **Specific AML controls.** These have a similar impact as general AML controls.

- **Inherent vulnerability variables.** Higher ratings increase the vulnerability of the product, thereby increasing the banking sector vulnerability; lower ratings decrease the banking sector vulnerability.

Each assessment worksheet includes the definition of the 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 support the 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 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 most 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.

As explained above Section 4 and Section 5 are related to Stage 1, while Annex provides detailed instructions on how to use the Excel file (Stage 2). During the sessions in 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 Reliable Identification Infrastructure*, and *Availability of Independent Information Sources* are included in every module of the tool, and are assessed at a national level. Their assessment rating should be consistent across all modules, and should be based on systematic and logical reasoning. Although it is sufficient for one WG to assess the ratings of these input variables, it is advised that both the National Vulnerability and Banking Sector Vulnerability WGs assess these variables. It will be useful to compare the assessment ratings assigned by the two groups and to resolve any conflicts that might occur. It is necessary to ensure that assessment ratings are agreed for these three input variables.

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 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 data and information from the previous five years, as only then may it be possible to discern relevant trends and cumulative amounts.

Table 1: 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 table 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 the general public or 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 each General AML Controls variable. Each assessment worksheet contains a description of the variable, the assessment criteria, brief guidance on how to support the assessment and a section to record the rating.

The General AML Control variables of this module relate to the strength of the general AML controls. These variables affect the vulnerability of all banking sector products, as well as the overall vulnerability of the sector. This assessment is sector-wide, therefore should consider all the banks within the sector. The General AML Control variables are as follows:

1. *Comprehensiveness of AML Legal Framework*
2. *Effectiveness of Supervision Procedures and Practices*
3. *Availability and Enforcement of Administrative Sanctions*

4. *Availability and Enforcement of Criminal Sanctions*
5. *Availability and Effectiveness of Entry Controls*
6. *Integrity of Banks' Staff*
7. *AML Knowledge of Banks' Staff*
8. *Effectiveness of Compliance Function (Organization)*
9. *Effectiveness of Suspicious Activity Monitoring and Reporting*
10. *Level of Market Pressure to Meet AML Standards (Optional)*
11. *Availability and Access to Beneficial Ownership Information*
12. *Availability of Reliable Identification Infrastructure*
13. *Availability of Independent Information Sources.*

In order to better understand how these variables impact the vulnerability of the banking sector, please refer to Figure 3.a.

At this stage, the assessment does not focus on vulnerability directly. The assessment is more about the quality, effectiveness, or level of these variables. Based on these inputs, vulnerability is determined by the module. For example, the assessment should rate the effectiveness of compliance function in the banks, not the impact of their effectiveness on banks' vulnerability to ML. This basic principle applies to all input variables.

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

Availability and Access to Beneficial Ownership Information, *Availability of Reliable Identification Infrastructure* and *Availability of Independent Information Sources* are input variables that are present in several modules of the tool, and are assessed at a national level. The assessment rating for these variables should be consistent across all modules. Although one WG assigning these ratings is sufficient, it is advised that both the National Vulnerability and Banking Sector WGs assess these variables. It is useful to compare the assessment ratings assigned by the two groups, and to resolve any conflicts that might occur. It is necessary to ensure that assessment ratings are agreed for these three input variables.

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 below. The table should be extended as necessary.

Name of the input 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:

Completing the Entry Page tab in the Excel file

The results of the General AML controls assessments should be filled out on the Entry Page tab in the Banking Sector Vulnerability Excel file. This should only be done after every variable has been assessed. Please refer to the Annex for detailed instructions on how to use the Excel file.

4.1.1. Comprehensiveness of AML Legal Framework

Variable description

This variable assesses whether a country has comprehensive laws and regulations regarding AML preventive measures and AML supervision of the banking sector.

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 banking sector.

Assessment criteria

A country has comprehensive AML laws and regulations in force within the banking sector if these laws and regulations:

1. Conform to the 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
    - Customer Due Diligence in case of correspondent banking, new technologies, and wire transfers
    - Reliance on Customer Due Diligence by third parties (including introduced business)
    - Suspicious Transaction Reporting
    - Licensing
    - Tipping-off and confidentiality
    - Internal controls, foreign branches, and subsidiaries
    - Regulation and supervision of financial institutions
    - Supervisory powers.
2. Largely comply with the revised Basel Core Principles (2012), particularly Principles 1, 2, 3, 4, 5, 9, 11, 13, 25, 26, and 29.

Possible sources of information and data

- Relevant laws, regulations, and enforceable guidance related to the items above
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff.

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 Procedures and Practices

Variable description

This variable assesses the effectiveness of AML supervisory procedures and practices for the banking sector. An effective supervisory regime is one that: (1) has a comprehensive legal and regulatory framework, which is supported by appropriate powers and is well resourced, and (2) employs a risk-based approach to on-site/off-site monitoring and inspection.

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

AML supervision procedures and practices are effective when the supervisory body:

- Is clearly identified in the laws and regulations, and 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 of the ML risks within the sector
- Has a sufficient number of trained staff
- Equips staff with the necessary skills and up-to-date knowledge for AML compliance examinations
- Has necessary resources to ensure AML compliance (such as technical capacity, budget, and tools)
- Carries out a comprehensive, risk-based supervisory program that consists of on-site and off-site components on both regularly scheduled cycles and periodic spot-checks (risk-based and as necessary)
- Reports and records 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 banking sector managements, 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 off-site supervision activities and findings
- Statistics on the number of banks actually inspected (on-site/off-site) and information as to the scope, frequency, and intensity of the inspections
- Statistics and information on the main findings of inspections (on-site/off-site)
- Interviews/consultations with bank supervisory authorities
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Surveys of bank managements and staff.

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 a country has a range of effective, proportionate, and dissuasive administrative sanctions applicable to natural or legal persons in cases of non-compliance with AML laws and regulations. Sanctions should be applicable not only to financial institutions including banks, but also to their directors and senior management. 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 a country takes administrative enforcement action against a bank, or individual members of bank management or staff, in cases of non-compliance with AML obligations. Consider the number of administrative actions that have been taken against banks and bank staff over the past few years for non-compliance with AML obligations.

Assessment criteria

The following criteria indicate if a country has effective, proportionate, and dissuasive administrative sanctions in place:

- Appropriate administrative sanctions are in place for noncompliance with AML obligations
- Administrative sanctions are sufficient to positively influence bank management and staff behavior (such as monetary penalties, administrative actions, removal of critical staff, and suspension/withdrawal of bank licenses).

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

- Most persons working in the banking sector believe that administrative action would be initiated in case of noncompliance with AML requirements.
- There is a record of administrative enforcement actions taken in the past by law enforcement authorities regarding noncompliance with AML requirements within the sector.

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

Possible sources of information and data

- Specific legal and regulatory provisions concerning administrative sanctions
- Statistics (by type) of past administrative enforcement actions taken by relevant authorities
- Information on the steps taken (or not taken) by banks to remedy infractions
- Interviews/consultations with bank supervisory authorities
- Interviews/consultations with banking sector representatives, including professional bodies and voluntary associations (which includes the forms of sanctions they enforce, such as disciplinary hearings or revocations of membership)
- Surveys of bank managements and staff.

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 a country has a range of effective, proportionate, and dissuasive criminal sanctions, which are applicable in cases of non-compliance with AML laws and regulations. This should include sanctions for serious and deliberate (or criminally negligent) breaches that can be ancillary to the money laundering offense. Sanctions should be applicable not only to financial institutions (including banks), but also to their directors and senior management. The more the criminal sanctions are effective, proportionate, and dissuasive, the more likely it is that management and staff members comply with AML laws and obligations.

This variable assesses not only legal frameworks, but also actual enforcement actions taken against a bank, or individual members of banks managements or staff, in cases of non-compliance with AML obligations.

Assessment criteria

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

- Appropriate criminal sanctions are in place for noncompliance with AML obligations.
- Persons in the banking industry regard the criminal sanctions regime as sufficiently dissuasive to positively influence individual behavior patterns.
- Criminal sanctions are also applicable for appropriate ancillary offenses to ML offenses.

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

- Most persons working within the banking sector believe that criminal enforcement action would be initiated in cases of noncompliance with AML requirements.
- There is a record of convictions, and criminal enforcement actions, that have been taken over the past years by law enforcement authorities regarding noncompliance with AML requirements in the sector. Consider the number of investigations, prosecutions, and convictions, as well as other available evidence on enforcement actions.
- Criminal enforcement against banks and their staff in regards to other financial crimes (such as fraud, etc.), may also give an insight into the perceptions of enforcement within the sector.

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 sector
- Statistics on criminal enforcement actions that have been carried out by foreign law enforcement (and other relevant authorities) against banks and individual members of staff, and whether (as well as in what form, and to what extent) the country provided informal/formal assistance to the investigation and prosecution
- Interviews/consultations with the bank supervisory authority, law enforcement agencies, and prosecution agencies
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Surveys of bank managements and staff.

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). 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 trained staff, and other resources with which to carry out their duties. Effective entry controls help to reduce money laundering vulnerability and ensures a higher level of compliance with AML requirements.

Assessment criteria

Entry controls are effective when the licensing body:

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

Possible sources of information and data

- Licensing and registration laws and regulations, policies, procedures (including application forms and supporting documentation), and manuals for supervisory staff
- Statistics on license applications received and actually granted
- Statistics and information on licenses not granted or later suspended or revoked for failure to meet AML controls
- Interviews/consultations with bank supervisory authorities
- Interviews/consultations with banking sector representatives (including professional bodies and volunteer associations)
- Surveys of bank managements and staff.

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 Banks' Staff

Variable description

This variable assesses whether bank staff acts with integrity. This means that the staff does not act in a willfully blind manner or collude with criminals or act corruptly. In addition, they take care to ensure that they do not become unwittingly involved (as "innocent agents") for criminals that seek to use their products including specialized knowledge and skills.

If bank staff members collude with criminals or undermine AML controls by acting corruptly, banks are vulnerable to money laundering abuse. Consider the effectiveness of staff vetting programs within the industry, the incidence of disciplinary action for breaching integrity-related rules, and the number of criminal cases against bank staff members.

Assessment criteria

Banks' staff is acting with integrity if the following criteria are met:

- Banks 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 the bank staff is low (but consider whether there is underreporting of incidences of integrity failure.
- There are appropriate mechanisms in place to protect bank staff against negative consequences resulting from reporting STR, or other actions complying with AML obligations.

Possible sources of information and data

- Relevant laws/regulations (including specific provisions on confidentiality mechanisms in place for the bank staff when reporting suspicious or other relevant transactions)
- Information on staff vetting and training programs
- Interviews/consultations with banking sector representatives, including professional bodies and voluntary associations (particularly internal control, or compliance units)
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff
- Findings of on-site/off-site AML examinations of banks
- Statistics on integrity breaches by bank staff and the disciplinary actions taken as a result
- Statistics on the number (and types) of administrative enforcement actions taken against banks and individuals working in the sector
- Statistics on criminal cases, including money laundering cases against bank staff
- Review of reports/records of internal control/compliance units at banks
- Historical data of incidents/breaches by bank staff (kept for operational risk management purposes)
- Banks' reputation on involvement in financial crimes, including tax evasion
- General level of integrity, or the operating environment in the country (e.g., Transparency International's Corruption Perception Index).

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 Banks' Staff

Variable description

This variable assesses how well the banks' staff knows and understands their AML duties and responsibilities.

Assessment criteria

Banks' staff have the required level of AML knowledge if:

- There are appropriate AML training programs and materials available to bank staff.
- Training programs are designed to ensure 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 bank conducts business with clients and professional intermediary firms in other jurisdictions, their knowledge should also extend to 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 those involving the misuse of the bank, its products and services, and specialized knowledge and skills of its staff.
- Staff members are aware of AML compliance, reporting procedures, and obligations.
- Staff members understand the legal consequences of AML compliance breaches.

Possible sources of information and data

- Relevant regulatory framework
- Interviews/consultations with banking sector representatives, including professional bodies and voluntary associations (particularly internal control units)
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff
- Findings of on-site/off-site AML examinations of banks
- Statistics and information on AML training activities by banks (hours of trainings, number of trainees, frequency of trainings, level and type of staff trained, mandatory/voluntary participation, etc.)
- Information on AML training programs and the training material of banks
- Statistics on AML trainings given by public authorities to banks.

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 banks have an effective compliance function that is comprehensive, risk-based, and well-resourced with an independent AML compliance function.

Assessment criteria

The banking sector possesses effective internal AML compliance functions if most banks:

- Have internal compliance programs that are commensurate to the level of risk, taking into account factors such as the volume and nature of the products provided, the client base profiles, the transaction patterns, and the cross-border nature of transactions
- Have appointed a sufficiently resourced and independent AML compliance officer at a senior management level
- Take disciplinary actions against their staff in cases of breaches of compliance policy
- Perform internal and/or external AML audits.

Possible sources of information and data

- Relevant regulatory framework in relation to the compliance function
- Information on the internal compliance function and policies of banks
- Findings of AML on-site inspections and off-site monitoring
- External (if any) and internal audit reports on the adequacy and effectiveness of compliance functions
- Statistics on the disciplinary actions taken by banks against their staff for breaching the compliance policy
- Statistics on new clients, declined business, or terminated business relationships based on recommendations from the compliance staff
- Interviews/consultations with bank supervisory authorities
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Surveys of bank managements and staff.

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 banks 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 rural bank with a single branch, while conversely; large banks will require more sophisticated systems. A good record-keeping system is a pre-requisite for an effective monitoring system. Therefore any problems and deficiencies in record keeping should be assessed under this variable.

Assessment criteria

If the following criteria are met, it indicates that banks have adequate and appropriate AML monitoring and STR reporting systems:

- Banks have information systems that enable and facilitate the monitoring of transactions of clients against their profiles.
- Transactional records are available in a format that facilitates AML screening and monitoring.
- The systems support banks in performing effective PEP screenings.
- The systems assist banks and bank staff to effectively identify and record all complex, unusual large transactions.
- The systems assist banks and bank staff to effectively identify and report suspicious transactions.

Staff should have a good understanding of the scope of their reporting obligations on suspicious transactions and activities, including what activities are covered or not covered under laws.

Possible sources of information and data

- Relevant regulatory framework in relation to AML monitoring, record-keeping, and STR reporting obligations
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff
- Findings of AML on-site/off-site examinations
- Information on quality and accessibility of banks' transaction records
- Findings of the supervision with regard to the effectiveness of the banks' STR reporting systems. (How many banks are compliant, how many are not compliant? How does this impact the overall effectiveness of the STR reporting system in the banking sector?)
- Statistics on the number and quality of STRs filed, including the numbers filed defensively (after being alerted to suspicious activity, or investigation by authorities)
- Statistics on the numbers of STRs relating to monitoring lapses originating from banks
- Statistics on the number of STRs by banks referred to law enforcement agencies
- Information on quality of STRs and STR system of banks
- Any other statistics on the outputs from AML monitoring systems in banks (for example, unusual transactions).

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. Level of Market Pressure to Meet AML Standards (Optional)

Variable description

This is an optional variable. It assesses whether (and if so, to what extent) market forces exert pressure on bank managements to have an effective AML compliance function. It addresses the pressures that exist outside of a country's legal and supervisory regimes; for instance, commercial pressure that is applied by commercial counterparts such as correspondent banks.

This variable is different from the other control variables in terms of being subject to policy decisions. The market pressure is determined by the domestic and international market forces and may not be easily and/or directly impacted by policy decisions and regulatory interventions.

Given this variable's limited impact on policy decisions, the WG may choose not to assess it.

Assessment criteria

If the following criteria are met, it indicates that market pressure on bank managements to meet international AML standards exists:

- Banks have cross-border correspondent relationships that they deem important and that require them to comply with international AML standards if they wish to maintain these relationships.
- Bank managements are sensitive to international and national AML-related reputational risks.

Possible sources of information and data

- Interviews/consultations with banking sector representatives (both within the country and any relevant external counterparts)
- Interviews/consultations with bank supervisory authorities (both within the country and any relevant external counterparts)
- Surveys of bank managements and staff.

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 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.

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 ☐

4.1.12. Availability of 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.

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 ☐

4.1.13. 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.

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 certain products. These factors are called inherent vulnerability variables. Each assessment worksheet contains the description of the variable, the assessment criteria, brief guidance on how to support the assessment, and an assessment section to record the decided ratings.

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. The vulnerability of a product will also depend on the availability of any additional AML control that is specific to that particular product. Product-specific AML controls are explained in Section 4.3.

This section provides guidance on seven inherent vulnerability variables.

Inherent vulnerability factors

The following input variables reflect the inherent vulnerability factors:

1. *Total size/value of the product*
2. *Average transaction size of the product*
3. *Client base profile of the product*
4. *Existence of investment/deposit feature for the product*
5. *Level of cash activity associated with the product*
6. *Frequency of international transactions involving the product*
7. *Other vulnerable factors of the product*

These seven inherent vulnerability input variables determine the vulnerability for each individual product. The assessment of these seven inputs should be performed for each product separately. Therefore, if the country is assessing 10 products, there are (7*10=) 70 variables that will need to be assessed.

Suggested list of bank products to assess

This suggested list of products has been designed to provide the WG with a starting point. The WG is encouraged to modify the list depending on the country context. If one or some of the products does not exist in the country, it can be deleted from the list, while other products that are important in the country context may be added.

Suggested list of products to assess:

1. Private banking
2. Retail deposits
3. Deposits of legal persons
4. Credit products for retail customers
5. Credit products for small and medium-size businesses
6. Credit products for large businesses
7. Current accounts
8. Wire transfers
9. Negotiable instruments
10. Trust and asset management services
11. Trade finance
12. Correspondent accounts
13. Electronic banking
14. Micro-credit products

The WG may decide to further break down some of the products, if it feels that different sub-categories within a product may pose different ML risks. For example, if the WG thinks that the client profile, cash-intensive use, or any other vulnerability factor of retail deposit accounts below USD 1,000 is different from the ones above USD 1,000, and it is not correct to assess them in the same basket, the WG may decide to have two separate categories.

The WG may also decide to include some other products that are important in the country context, such as payable through accounts, brokered deposits, Trust and Company Provision Services, etc. As far as possible, all the significant products and any new, unique, unusual products – even if their volume is not necessarily significant – should be included in the assessment.

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

The results of the assessments of the vulnerability of specific products need to be entered into the **Entry Page (Products) tab** of the Banking Sector Vulnerability Excel Module. This should be done only after the assessments of all the variables have been completed. Please refer to the Annex for detailed instructions on how to use the Excel file.

4.2.1. Total size/value of the product

Variable description

This variable assesses the total size/value of a particular product in the banking sector. The total size/value of a particular product in the banking sector is indicative of the level of ML vulnerability it can introduce into the sector if any associated risks are not mitigated. The objective of this indicator is to assess the importance of a particular product within the banking sector, in comparison to other products offered by the sector.

A higher size/value of the product in the sector will make it easier to camouflage the dirty transactions for criminals and more difficult for the institutions to red flag and detect these.

Assessment criteria

The most appropriate indicator of the total size/value of a product in the banking sector depends on the nature of the product being assessed. For some products, the size of the assets or liabilities associated with the product can be used as an indicator of the total size/value. For example, for retail deposits, the total amount of the retail deposits on the liabilities side of banks' balance sheets can be used as an indicator of the total size/value; while for some services or service channels (such as correspondent accounts, electronic banking or wire transfers), it will be more meaningful to use the total amount of fund flows. It may be appropriate to use assets managed as an indicator for trust and asset management services.

If banks attract significant funds from foreign clients for a particular product and such funds are placed elsewhere and are not reflected in their balance sheets, it may be more appropriate to use total assets managed as an indicator of the total size/value for such products.

The actual number of transactions and amounts involved may be very difficult to determine. What is required is a judgment as to whether or not the product is significant in the sector. Consideration may also be given to the number of providers of the product, the relative number of the specific product compared to the total number of products provided and the total size/value of the product, compared to the contribution that the banking sector makes to the GDP.

Possible sources of information and data

- Data on total assets and liabilities associated with the assessed product
- Data on total turnover associated with the assessed product
- Data on total assets managed associated with the assessed product
- Data on total amount of fund flows associated with the assessed product
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff
- Interviews with and data compiled by private sector research or consulting firms.

Additional guidance

During the assessment, supervisory agencies need to refer to the aggregate balance sheet of the banking sector. While assessing the total size/value of a product, please try to decide whether it is significant or not. If it is significant, rate it as high; if it is not significant, rate it as low. If you think that it is moderately significant, rate it as medium.

4.2.2. Average transaction size of the product

Variable description

This variable assesses the average transaction size of a particular product. Products that are customarily used to process large transactions are more prone to attract the attention of money launderers with large amounts to launder.

Assessment criteria

The most appropriate indicator for the average transaction size of a particular product is the modal value of the transaction size of the product during a particular period of time.

Once the average transaction size has been identified, the identified amount needs to be mapped to the assessment scale, which ranges from Low to High. Identifying a benchmark will be helpful for this assessment.

The average transaction size of a particular product is high when it tends to exceed the average transaction size involved in a banking product like such as the current accounts of retail bank customers, as it is a product offered by the banking sector in almost all countries. Consider using the average transaction size for current accounts of retail bank customers as the benchmark, which corresponds to the midpoint on the assessment scale. The assessment ratings for all the other products will be determined relative to this benchmark.

An alternative benchmark can be the modal salary amount in the country, which would be considered a regular value for a transaction for banks. Most of the government and private sector employees will receive their salaries in their bank accounts. This amount would correspond to the midpoint on the assessment scale. The assessment ratings for all the other products will be determined relative to this benchmark.

Another alternative benchmark can be the amount of the monthly GDP per capita of the country. This amount would correspond to the midpoint on the assessment scale. The assessment ratings for all the other products will be determined relative to this benchmark.

Possible sources of information and data

- Data on transactions that make it possible to determine the value of transactions of the specific product. This should include data from all banks, or a few banks that are representative of the sector, for a specified period of time.
- Data on the modal monthly salary amount in the country.
- Data on the amount of monthly GDP per capita for the country.
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations).
- Interviews/consultations with bank supervisory authorities.
- Interviews with and data compiled by private sector research or consulting firms.
- Surveys of bank managements and staff.

Additional guidance

The objective of this indicator is to compare the average transaction size for various products. The products with very low average transaction size will be less convenient for money launderers since laundering large amounts of money with transactions involving small amounts would require a very large number of transactions. On the other hand, a small number of transactions using a service /product which characteristically involves transactions of large amounts can facilitate the laundering of large amounts of dirty money. To assess the average transaction size, the authorities will probably need to collect the relevant data from the banks, since such data tend not to be among the financial data regularly being reported by the banks to supervisory authorities.

If possible, this analysis should cover the data of the last full year (to take into account seasonal fluctuations) and all the bank branches. If not possible, this analysis can be limited to a few banks, which are representative of the sector, or over a shorter period of time (such as six months).

The concentration statistics collected by banks (for the purpose of monitoring concentration risk) can form a good indicator of the average transaction size, particularly of deposits and loans.

4.2.3. Client base profile of the product

Variable description

This variable assesses whether the type of client that generally uses the product being assessed increases the risks of money laundering abuse of these products.

Assessment criteria

The client base profile should be assessed as carrying a higher risk if it involves:

- Domestic/International PEPs
- High net worth individuals
- Nonresident 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
- Businesses with complex, non-transparent ownership structure
- Clients through introduced business or correspondent banking, particularly from unregulated professional intermediaries or regulated intermediaries in jurisdictions with low AML controls.

Possible sources of information and data

- Regulatory framework for risk-based classification of customers
- Regulatory framework for identifying and monitoring PEPs
- Any product-wise data on PEPs and other higher risk customers
- Banking sector data on international wire transfers/transactions
- Banking sector data on transactions with high-risk jurisdictions
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff
- Criminal data including ML cases where a product was used for ML by high-risk customers
- Statistics on STRs originating from banking sector with regard to high-risk customers
- Interviews with and data compiled by private sector research or consulting firms.

Additional guidance

While assessing the client base profile for each product, please assess whether this product is being used by the customers who pose a higher money laundering risk, when compared to standard customers. These high-risk customers will include politically exposed persons (PEPs), non-residents, high-net-worth individuals. It would be useful to look at the geographical breakdown of the transactions of clients. Many banks categorize transactions based on high-risk jurisdictions as higher risk for the purpose of screening and monitoring the transactions and to identify suspicious transactions. Transactions associated with high-risk jurisdictions are likely to be more vulnerable to money laundering as adequate AML controls are likely not in place and it is easier for criminals to move illicit funds to and from these jurisdictions into the global financial system. To assess this variable, financial institutions 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, banks may not be able to provide any information.

In many countries, the resident status of a bank customer is recorded during the process of establishing the business relationship. Thus banks should be able to identify non-resident clients, and determine which kinds of products they use. A more advanced analysis that is based on the countries that such non-resident clients originate from will provide further insight into the risk levels of various nationals.

In some cases, the nature of the product will determine the client base profile. For example, the client base profile of private banking would be high net worth individuals. While assessing this indicator, please consider the likelihood of criminals preferring this product over other products in the sector. If the likelihood is high, the assessment rating for the client base profile for this product should be relatively high.

Assessment of this indicator will require judgment if the country does not have appropriate mechanisms to identify and monitor high-risk customers (including PEPs). If there is no data that can support the assessment, the WG needs to consider the worst-case scenario and be conservative in its assessment.

One of the multiple choices of this item in the Excel file is Not Analyzed. Please note that, the Excel file penalizes this, since the lack of ability to analyze the client profile will pose a risk in itself.

4.2.4. Existence of investment/deposit feature for the product

Variable description

This variable assesses whether a product allows for the investment/deposit of funds into the financial system. In general, products that allow for the investment/deposit of funds are more vulnerable to ML than others, where the client borrows funds from a bank. For example, low-value retail loans are much less vulnerable to ML than deposit products. (This does not mean that credit products are not vulnerable to ML. High-value loans, especially, may be abused for ML purposes through the use of collateral or mingling of dirty money in the sums to be repaid.)

Assessment criteria

The extent of vulnerability to ML abuse for a particular product due to the availability of investment/deposit feature is dependent on whether such feature has extensive or limited functionality. For some products (such as private banking), an investment/deposit feature is prominent, and has extensive functionality due to the large sums of funds involved. This makes them more vulnerable to money laundering abuse than other products, such as micro-deposit products, which have limited investment/deposit functionality due to the small amount of funds being deposited, making them unattractive to money launderers.

The WG needs to analyze the availability of investment/deposit feature for various products. The more the functionality of such a feature in the product, the more vulnerable to ML it is.

Possible sources of information and data

- Bank product manuals
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Interviews with and data compiled by private sector research or consulting firms
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff
- Criminal data, including ML cases where a product was used for ML due to the availability of an investment/deposit feature.

4.2.5. Level of cash activity associated with the product

Variable description

This variable assesses whether the product allows for the use of cash that could increase the risk of money laundering abuse of a particular product.

Assessment criteria

Assess whether the product allows for the use of cash. If so, the product being assessed will be more vulnerable to money laundering. The more the product is cash-based, the more vulnerable to ML it is likely to be.

Possible sources of information and data

- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff
- Criminal data, including ML cases where a product was used for ML due to the possibility of transacting in cash
- Interviews with and data compiled by private sector research or consulting firms.

4.2.6. Frequency of international transactions involving the product

Variable description

This variable assesses the frequency of international transactions associated with a product that could increase the risk of money laundering abuse for that particular product.

Assessment criteria

If the product involves international wire transfers and other international transactions, it can be vulnerable to ML. The higher the number of international transactions involving a product, the more vulnerable it is to ML.

Higher frequency of internal transactions in a particular product will allow criminals to better camouflage their international money laundering operations.

Possible sources of information and data

- Banking sector data on international transactions, organized by product
- Number of STRs filed in respect of these products
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Interviews with and data compiled by private sector research or consulting firms
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff
- Criminal data, including ML cases where a product was used for ML and involved international transactions.

Additional guidance

The objective of this indicator is to distinguish the vulnerabilities of several bank products based on the frequency of international transactions in the course of the delivery to a client.

Banking sector data on international transactions relating to various products should be preferably on a consolidated basis taking into account data from all the banks. If possible, this analysis should cover the data of the last full year (to take into account seasonal fluctuations) and all the bank branches. If that is not possible, the analysis can be limited to one or a couple of branches which are representative of the sector, or over a shorter period of time (such as one month).

4.2.7. Other vulnerable factors of the product

Variable Description

This variable assesses whether there are any additional factors that render a bank vulnerable to the risk of money laundering.

Assessment criteria

The presence of the following typical factors may increase the ML vulnerability of the product:

- Possible anonymous/omnibus use of the product
- Indicators in ML typologies of abuse of the product
- Significant use of the product in tax evasion, or fraud schemes
- Difficulty in tracing the transaction records of the product
- Significant non-face-to-face use of the product
- Other vulnerable factors (e.g., the product is delivered/marketed through agents).

Possible sources of information and data

- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff
- Criminal data, including ML cases where a product was used for ML
- Data on statistics and qualitative information from MLA and formal or informal information/intelligence sharing requests from supervisory authorities, law enforcement, the FIU, tax, and other relevant authorities
- Interviews with and data compiled by private sector research or consulting firms

Additional guidance

Please note that existence of one or a few of these factors may render a product vulnerable to money laundering.

Anonymous/omnibus use of the product: Assess whether anonymous use of the product is possible. Also please consider whether the beneficial owner of the transaction is always identified. Does the product allow for omnibus use (where an investor known to the bank uses the product on behalf of several investors or a pool of investors who are unknown to the bank)? Omnibus transactions are vulnerable to money laundering, as the beneficial owner(s) of the funds involved in the transaction is/are not known. Bank customers execute the transaction on behalf of others. The real owners are not known and hence not subjected to customer due diligence.

Existence of ML typologies on the abuse of the product: Assess whether the product is known for abuse for ML purposes. This does not need to be in specific to the country. Global typologies can be relevant, regardless of whether it was detected or not in the country.

Use of the product in fraud or tax evasion schemes: Assess the use of the product in fraud or tax evasion schemes. For this purpose, it may be useful to refer to crime and tax data to find products that are considered most vulnerable. Tax evaders may purchase and utilize a system of nominee entities; sham trusts and related domestic and foreign bank accounts especially in high-risk jurisdictions. Use of the product in tax evasion or fraud schemes may indicate a vulnerability to ML abuse as well.

Difficulty in tracing the transaction records of the product: Please assess whether transactions executed in the course of delivery of a product have been properly recorded, and whether access to those records can be readily obtained. The difficulty in tracing the records would depend on the quality of banks AML record-keeping systems. For example, difficulty in tracing the records renders the use of digital cash vulnerable to ML.

Non-face-to-face use of the product: Availability of non-face-to-face initiation of business relationship with respect to a product raises ML vulnerability. Even in the case of traveler's checks or OTC derivatives, 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 account holder. These controls need to be assessed in the next indicator under the specific AML controls of that particular product.

Any other vulnerable factors (e.g., the delivery of the product through agents): Please provide information about any other factor that may render a particular product vulnerable to money laundering; for example, the use of agents. Delivery of the product through agents may increase the ML vulnerability of the product due to weak AML systems of the agents. If this is the case, *Other Vulnerable Factors* of the product need to be assessed as high. To limit vulnerability, agents have to be subjected to adequate AML controls and supervision by the principal bank. AML controls on agents need to be taken into account, not in *Other Vulnerable Factors* but in *Specific AML Controls* assessment for the product.

Summary of the assessment of products:

Considering the assessment criteria and guidance please assess the inherent vulnerability variables associated with the product. For each product, please check (✓) the appropriate option in the table below. The list of products may be amended as needed.

		1. Private banking	2. Retail deposits	3. Deposits of legal persons	4. Credit products for retail customers	5. Credit products for SMS businesses	6. Credit products for large businesses	7. Current accounts	8. Wire transfers	9. Negotiable instruments	10. Trust and asset management srv.	11. Trade finance	12. Correspondent accounts	13. Electronic banking	14. Micro credit products	15.	16.	17.	18.	19.	20.
Total size/value	High																				
	Medium High																				
	Medium																				
	Medium Low																				
	Low																				
	Not Analyzed																				
Average transaction size	High																				
	Medium High																				
	Medium																				
	Medium Low																				
	Low																				
	Not Analyzed																				
Client base profile	Very High Risk																				
	High Risk																				
	Medium Risk																				
	Low Risk																				
	Very Low Risk																				
	Not Analyzed																				
Existence of investment/deposit feature	Available and Prominent																				
	Available																				
	Available but Limited																				
	Not Available																				
Level of cash activity	High																				
	Medium High																				
	Medium																				
	Medium Low																				
	Low																				
	Does Not Exist																				
	Not Analyzed																				

Summary of the assessment of products:

Considering the assessment criteria and guidance please assess the inherent vulnerability variables associated with the product. For each product, please check (✓) the appropriate option in the table below. The list of products may be amended as needed.

			1. Private banking	2. Retail deposits	3. Deposits of legal persons	4. Credit products for retail customers	5. Credit products for SMS businesses	6. Credit products for large businesses	7. Current accounts	8. Wire transfers	9. Negotiable instruments	10. Trust and asset management srv.	11. Trade finance	12. Correspondent accounts	13. Electronic banking	14. Micro credit products	15.	16.	17.	18.	19.	20.
Frequency of international transactions		High																				
		Medium High																				
		Medium																				
		Medium Low																				
		Low																				
		Does Not Exist																				
		Not Analyzed																				
Other vulnerable factors	Anonymous omnibus	Available																				
		Not Available																				
	ML typologies	Significant																				
		Exist																				
		Exist but Limited																				
		Does Not Exist																				
	Abuse in fraud or tax schemes	Significant																				
		Exist																				
		Exist but Limited																				
		Does Not Exist																				
	Difficulty in tracing records	Records not available																				
		Difficult/Time Consuming																				
		Easy to trace																				
	Non-face-to-face	Available and Prominent																				
		Available																				
		Available but Limited																				
		Not Available																				
	Other	High																				
		Medium High																				
		Medium																				
		Medium Low																				
		Low																				
		Not Analyzed																				
		Does Not Exist																				

4.3. Assessment Worksheet for the Product-Specific AML Controls

Certain products are inherently more vulnerable to money laundering than others. This increased vulnerability may arise from characteristics of the product, such as the availability of anonymous use, non-face-to-face interactions, and frequent use of cash or from clients such as PEPs or high-net-worth individuals who typically use the product. To assess whether the incidence of such products affect the overall vulnerability of the sector, a separate assessment may be warranted. This assessment should consider any additional AML controls (in addition to general AML controls) that may be in place for the product. This is reflected in the variable *Availability of Product-Specific AML Controls,* which refers to controls designed for and applied to one particular product. For example, in addition to a generic list of red- flag indicators (for suspicious activity), the banking sector may have some specific red- flag indicators that focus on private banking; or they may require additional customer identification or monitoring procedures for private banking. These additional AML controls would reduce the vulnerability arising from private banking, and help reduce the overall vulnerability of the banking sector.

For some products, there may be no need for specific AML controls, as the general AML controls are considered adequate. In other words, specific AML controls are needed only if there are some particular risks that cannot be addressed by the general AML controls. Not having specific AML controls for all products is, therefore, not necessarily a problem.

Availability of product-specific AML controls

Variable description

This variable assesses whether appropriate specific AML controls are in place to manage any potential money laundering risk that may occur in the delivery of a particular product in the banking sector.

Specific AML controls are controls that are applied on top of the standard/general AML controls to all the products offered by the banks. Banks that implement specific AML controls may reduce their vulnerability to money laundering.

Assessment criteria

Specific AML controls for a product are in place if:

- Banks generally implement an effective, risk-based approach to AML.
- Banks regard the product as one that poses a higher ML risk and therefore apply specific AML controls.

Possible sources of information and data

- Regulatory framework for specific AML controls (please specify references to particular products)
- Data/information on the use of specific AML controls for a product from the sector
- Findings of AML on-site/off-site examinations
- Interviews/consultations with banking sector representatives (including professional bodies and voluntary associations)
- Interviews with and data compiled by private sector research or consulting firms
- Interviews/consultations with bank supervisory authorities
- Surveys of bank managements and staff.

Additional guidance

If the product is not subject to any specific AML controls, please select the option *Only General AML Controls exist.* For many products, general AML controls may be adequate for risk mitigation. Not having specific controls would not necessarily constitute a problem for a product, particularly for one with low or medium ML vulnerability. Existence of specific AML controls for all the products may indicate a high level of ML vulnerability for the banking sector. It is unlikely that all products require specific AML controls. Some products require only general AML controls and do not need specific AML controls because of low or medium ML vulnerability. One of the objectives of the product risk assessment is to identify whether the product needs specific AML controls or not.

While assessing the need for specific AML controls for a product, the WG should first assess the ML vulnerability of the product and understand the main cause of the vulnerability. For example, if a product is highly vulnerable to ML due to the use of agents, specific AML controls should be introduced only for the use of agents. These specific AML controls for agents will help to reduce the vulnerability of the product.

Specific AML controls may be required by law/regulations, or banks may apply them voluntarily. As far as possible, during the assessment, the WG needs to take into account the situation of the entire banking sector. In the cases where specific AML controls are required by law/regulations, the assessment needs to consider the effectiveness of the implementation of those specific AML controls.

Please note that specific AML controls do not refer to other controls aimed at the elimination of credit risk, fraud risk, risk arising from liquidity or treasury, or other operational risks. As their objective is different, these types of controls may not always contribute to the elimination of ML risks. For example, credit controls for loans may focus on the wealth and income of the client and may pay less attention to the source of funds. The WG can take into account these types of controls in limited conditions only, namely when they contribute to reducing ML risks.

As an example, in private banking, the specific AML controls may include the following:

- Risk-based categorization of the clients
- Risk-based categorization of transactions
- Risk-based ongoing monitoring
- Enhanced CDD
- Additional guidance and training to the relevant staff on red flag indicators those are specific to private banking
- Additional internal AML controls
- Additional off-site and on-site AML examination procedures.

Summary of the assessment of products:

Considering the assessment criteria and guidance please assess the availability of specific AML controls associated with the product. For each product please check (✓) the appropriate option in the table below. The list of products may be amended as needed.

		1. Private banking	2. Retail deposits	3. Deposits of legal persons	4. Credit products for retail customers	5. Credit products for SMS businesses	6. Credit products for large Businesses	7. Current accounts	8. Wire transfers	9. Negotiable instruments	10. Trust and asset management services	11. Trade finance	12. Correspondent accounts	13. Electronic banking	14. Micro credit products	15.	16.	17.	18.	19.	20.
Availability of specific AML controls	Exist and Comprehensive																				
	Exist but Limited																				
	Only General AML Controls																				

5. DESCRIPTION OF THE INTERMEDIATE VARIABLES

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

VARIABLE	DESCRIPTION
Quality of AML Supervision	This variable assesses whether the banking sector has a comprehensive AML supervision regime supported by appropriate powers, staff and other resources. This variable depends on the: • *Effectiveness of Supervision Procedures and Practices* • *Availability and Enforcement of Administrative Sanctions.*
Commitment and Leadership of Banks' Managements	This variable assesses bank managements' commitment and leadership in AML, and how management is influenced by the following variables: • *Availability and Effectiveness of Entry Controls* • *Quality of AML Supervision* (intermediate variable) • *Availability and Enforcement of Criminal Sanctions* • *Level of Market Pressure to Meet AML Standards (optional).*
Quality of Internal AML Policies and Procedures	This variable assesses the quality of banks' internal AML policies and compliance procedures, which depends on the: • *Comprehensiveness of AML Legal Framework* • *Commitment and Leadership of Banks' Managements* (intermediate variable) • *Effectiveness of Compliance Function.*
Compliance of Banks' Staff	This variable assesses the compliance level of banks' staff with the AML legal framework and their institutional obligations. This variable considers how this is influenced by factors such as the: • *Quality of AML Supervision* (intermediate variable) • *Availability and Enforcement of Criminal Sanctions* • *Effectiveness of Compliance Function* • *Integrity of Banks' Staff* • *AML Knowledge of Banks' 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, as well as the capacity 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 of Reliable Identification Infrastructure* • *Availability of Independent Information Sources* • *Availability and Access to Beneficial Ownership Information.*
Quality of Banks' Operations	This variable assesses the quality of banks' operations in preventing the abuse of banking products for money laundering. This variable depends on the: • *Commitment and Leadership of Banks' Managements* (intermediate variable) • *Compliance of Banks' Staff* (intermediate variable) • *Effectiveness of Suspicious Activity Monitoring and Reporting* • *Quality of CDD Framework* (intermediate variable).
Quality of General AML Controls	This variable assesses the quality of general AML controls in the banking sector, which are the standard AML controls applied to all products. This variable depends on the: • *Quality of Internal AML Policies and Procedures* (intermediate variable) • *Quality of Banks' Operations* (intermediate variable).

VARIABLE	DESCRIPTION
Quality of Specific AML Controls (for a product)	This variable assesses the effectiveness of the specific AML controls, which are the enhanced controls designed specifically for the bank products, are effective when they prevent and detect money laundering activities relating to a certain product. This variable depends on the: • *Availability of Product-Specific AML Controls* • *Quality of Banks' Operations* (intermediate variable) • *Quality of General AML Controls* (intermediate variable).
Product AML Controls	This variable assesses the overall effectiveness of all the AML controls together for a product in preventing and detecting money-laundering activities. This variable is affected by the: • *Quality of Specific AML Controls* (for a product) (intermediate variable) • *Quality of General AML Controls* (intermediate variable).
Product Inherent Vulnerability	This variable assesses the susceptibility of a particular banking product to money laundering solely based on inherent factors of the product without taking into account its AML controls. A banking product is inherently vulnerable when its characteristics render it open to abuse for money laundering. This relies on inherent vulnerability variables, namely: • *Total size/value of the product* • *Average transaction size of the product* • *Client base profile of the product* • *Existence of investment/deposit feature for the product* • *Level of cash activity associated with the product* • *Frequency of international transactions involving the product* • *Other vulnerable factors of the product.*
Product Vulnerability	This variable assesses the overall susceptibility of a particular banking 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: • *Product Inherent Vulnerability* (intermediate variable) • *Product AML Controls* (intermediate variable). **The ratings of all the product vulnerability assessments determine the vulnerability of the banking sector.**

ANNEX – INSTRUCTIONS FOR USING THE EXCEL FILE (MODULE 3)

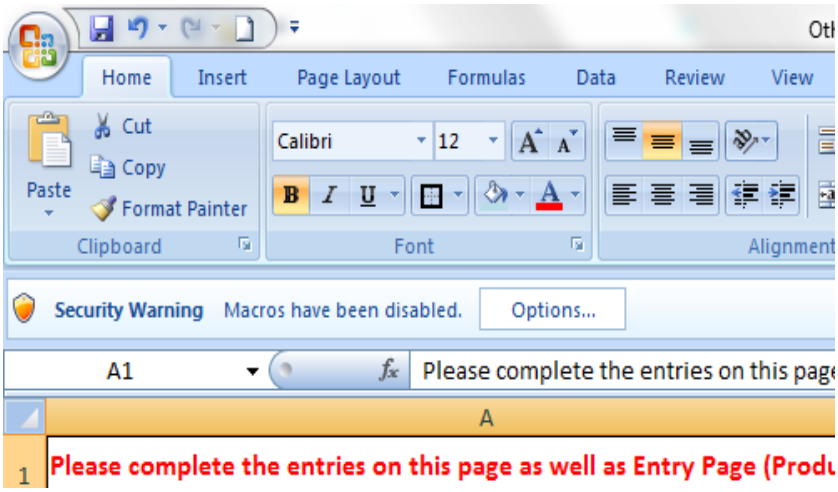
At this stage, the input variables have been assessed, and assigned a rating. These ratings now need to be entered into the Excel file. This Annex provides step-by-step instructions for using the Excel file to assess the vulnerability of the banking sector.

- 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

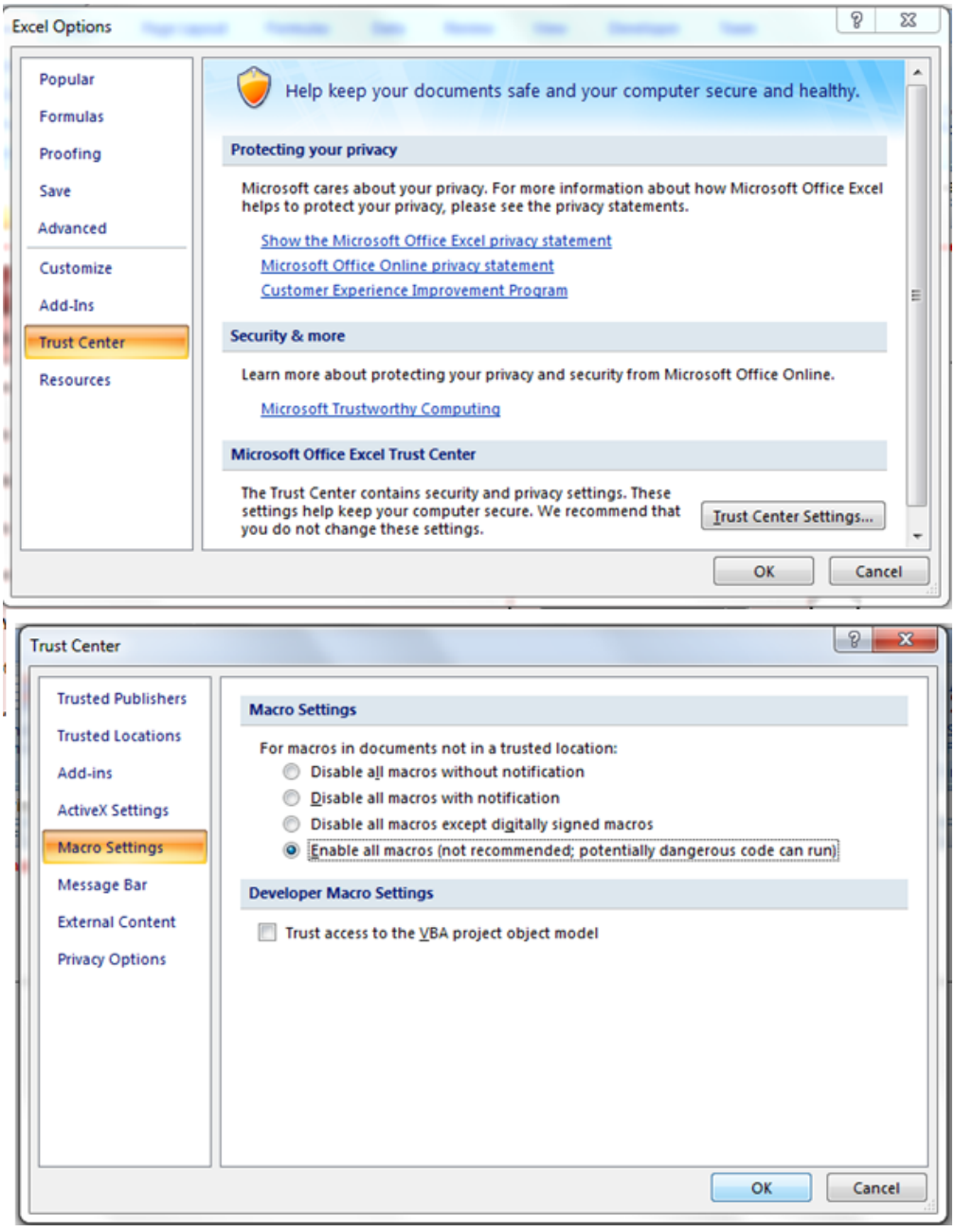
After opening the Excel file, first enable macros. A security warning will appear in the top left-hand corner of the first tab (Entry Page), warning you that macros are disabled – as shown in Figure 4.a. Click on the **Options** icon and select the **Enable this Content** option. Click **OK**, or (depending 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**.

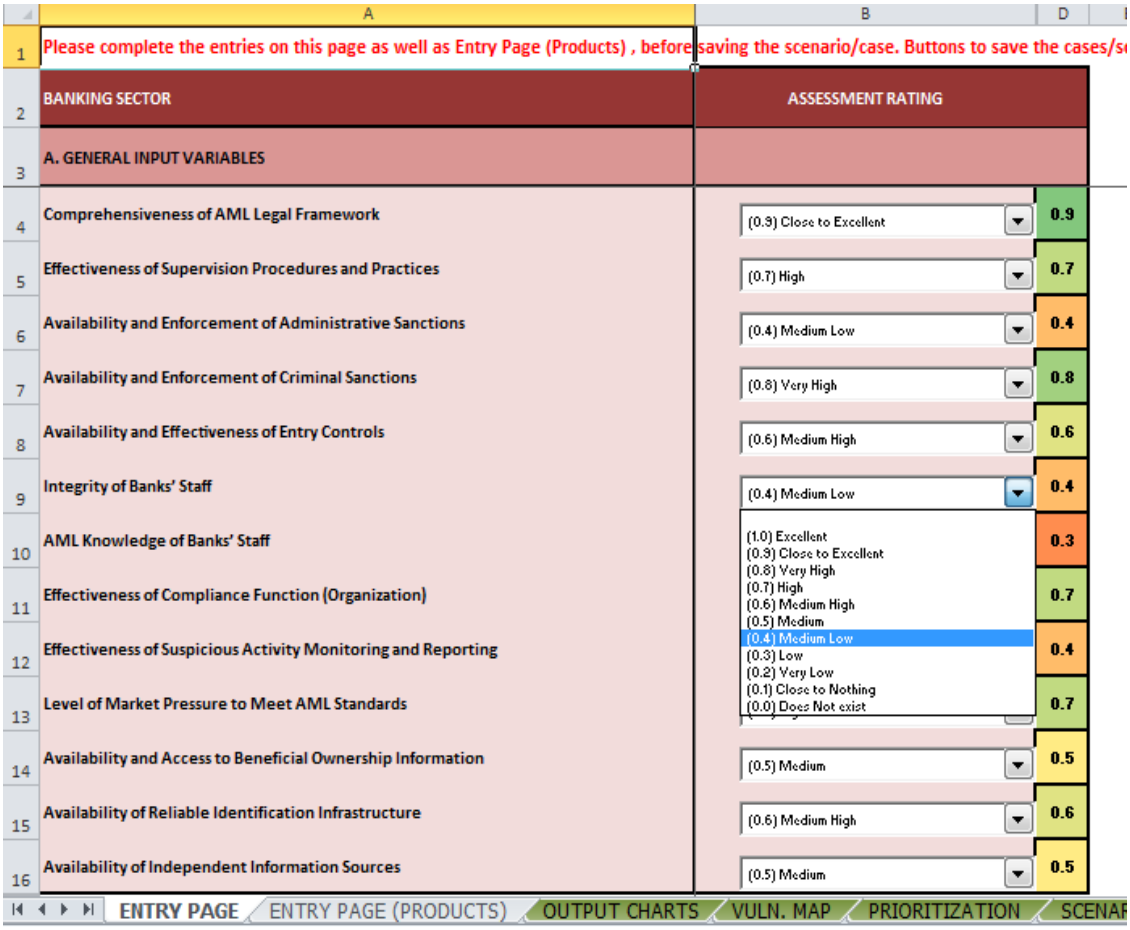
Figure 4.b: **Macro settings**



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 lower banking sector vulnerability. 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.

Figure 5: **Entries for general input variables (in the Entry Page tab)**



To complete the assessment, assessment ratings need to be entered for all thirteen general input variables. *Level of Market Pressure to Meet AML Standards* is an optional variable, and if you choose not to assess it, select the option **Does Not Apply** (do not choose the option **Does Not Exist**). If the rating for any general input variables has not been entered, a warning that the file is incomplete will appear in row 18 of the Entry Page tab.

Bear in mind that the assessment of the general input variables is applicable to the entire banking sector, and will influence the vulnerabilities of all the products.

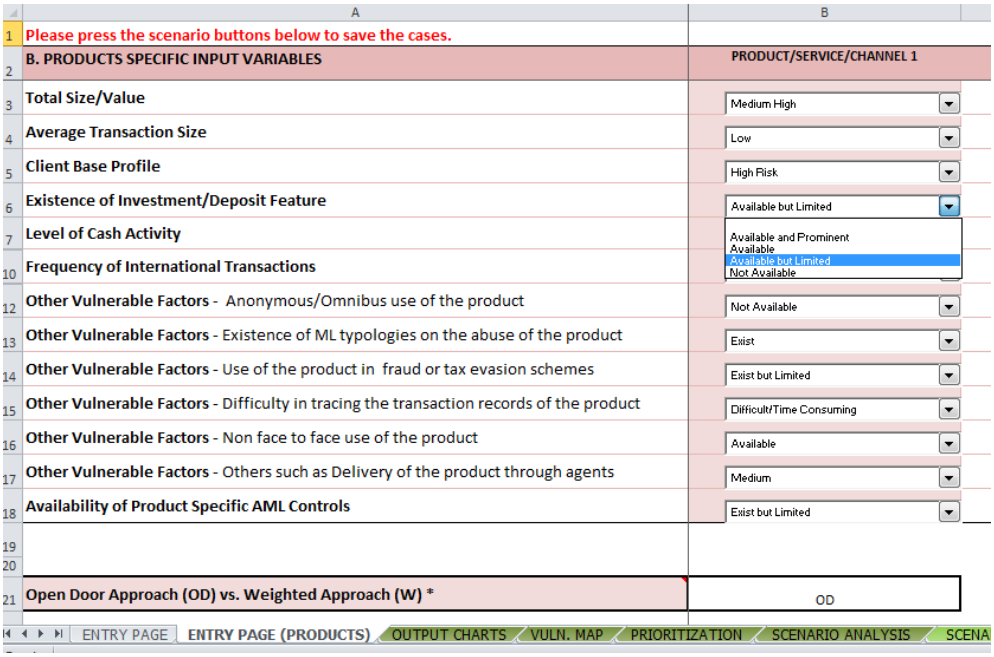
Step 3: Entries for inherent vulnerability variables and specific AML controls (in the Entry Page (Products) tab)

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 (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/Channel #, and enter the name of the product to be assessed.

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 (see Figure 6).

The Excel file is designed to facilitate the assessment of up to 20 products. However, if needed, you can use a second file to assess additional products. In this case, to assess sector vulnerability, the Working Group (WG) should use a third file as the master file. This master file should include only the 20 products with the highest vulnerability in two working files.

Figure 6: Entries for product-specific input variables (in the Entry Page (Products) tab)



The chosen specific input variable ratings for each of the assessed products needs to be entered to complete the assessment. 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 19 of the Entry Page (Products) tab.

The WG 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 banking sector on the basis of the weighted averages of all the products assessed. Weights are determined by the total size/value entries of each of the assessed products.

(2) **The Open Door Approach.** This approach calculates the overall banking sector vulnerability score, 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 sector vulnerability, the Open Door Approach focuses on the products with higher vulnerability.

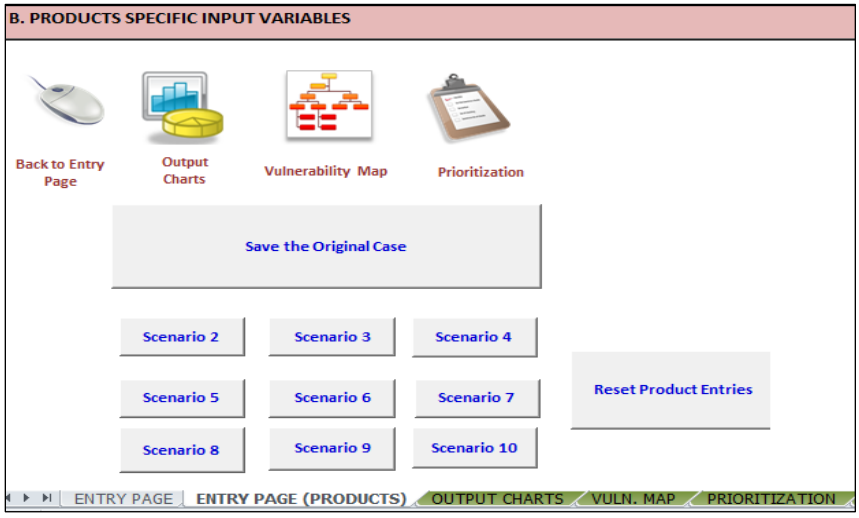
The Open Door Approach has been chosen as the default option in the Excel file. Thus, the entry in cell B 21 is "OD" (see Figure 6). If you prefer the Weighted Average Approach, switch to the weighted average option by entering "W" in this cell.

In order to compare the outcomes of the two approaches, it is suggested that the WG 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 sectoral money laundering vulnerability 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 inherent vulnerability variables and the specific AML control variables for all products have been entered, save the entries by clicking the **Save the Original Case** icon on the Entry Page (Products) tab – as shown in Figure 7. 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 7: Icons on the Entry Page (Products) tab



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:

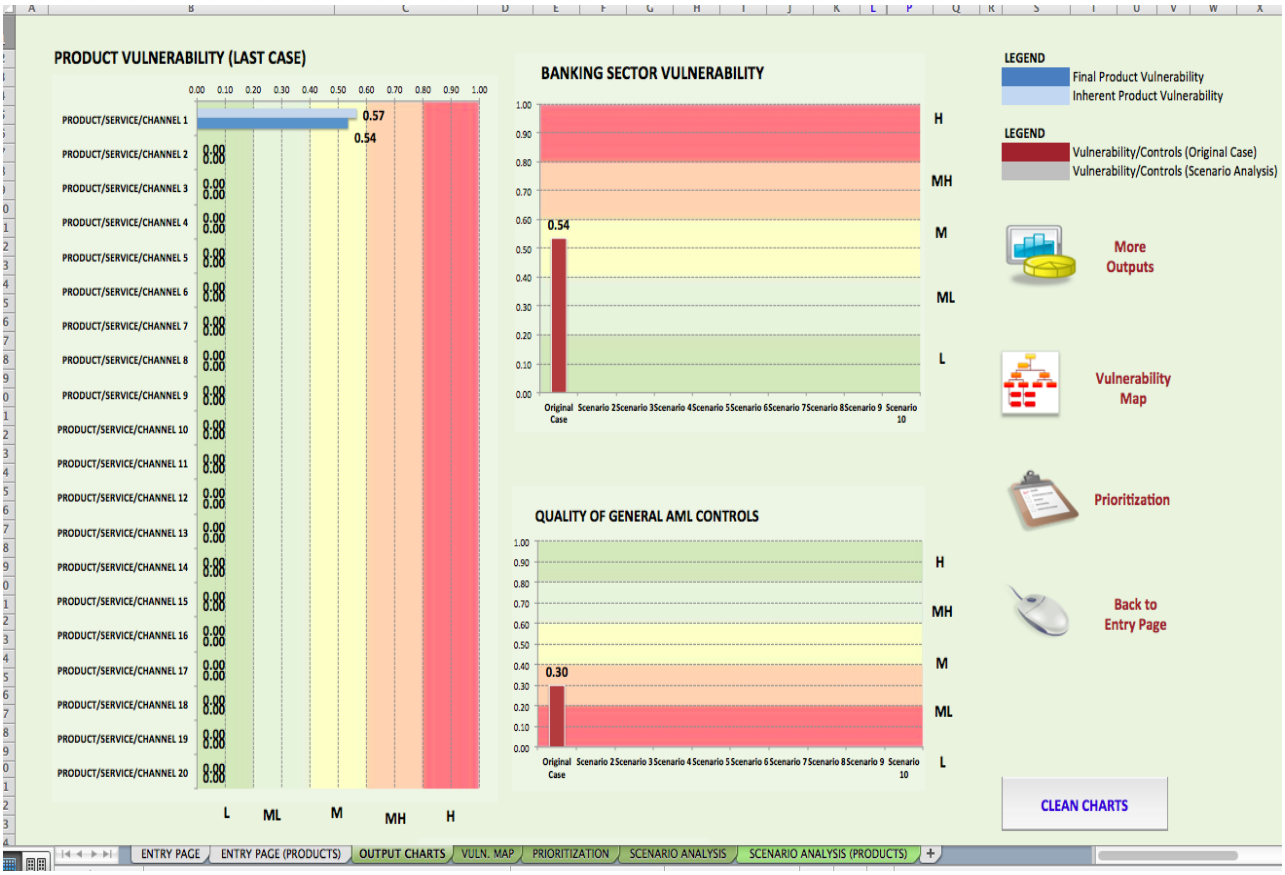
1. Output Charts
2. Vulnerability Map (Network Diagram)
3. Prioritization.

1. *Output Charts tab*

The Output Charts tab shows the banking sector's vulnerability, the vulnerability of each assessed product, and the assessment results for intermediate variables such as *Quality of General AML Controls,* in a visual format (see Figure 8). For output charts, click on the **Output Charts** icon in the Entry Page (Products) tab to view the assessment results (as shown in Figure 7).

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 8: Output Charts



For both the product vulnerability chart and the banking sector vulnerability chart, a higher score implies a higher vulnerability to ML. Similarly, a higher product vulnerability score increases the vulnerability score of the banking sector.

On the other hand, for intermediate variables that relate to controls (such as *Quality of General AML Controls, Quality of CDD Framework*, and *Compliance of Banks' Staff*) a higher score indicates a higher combating ability, which lowers the vulnerability of the banking sector to ML.

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.

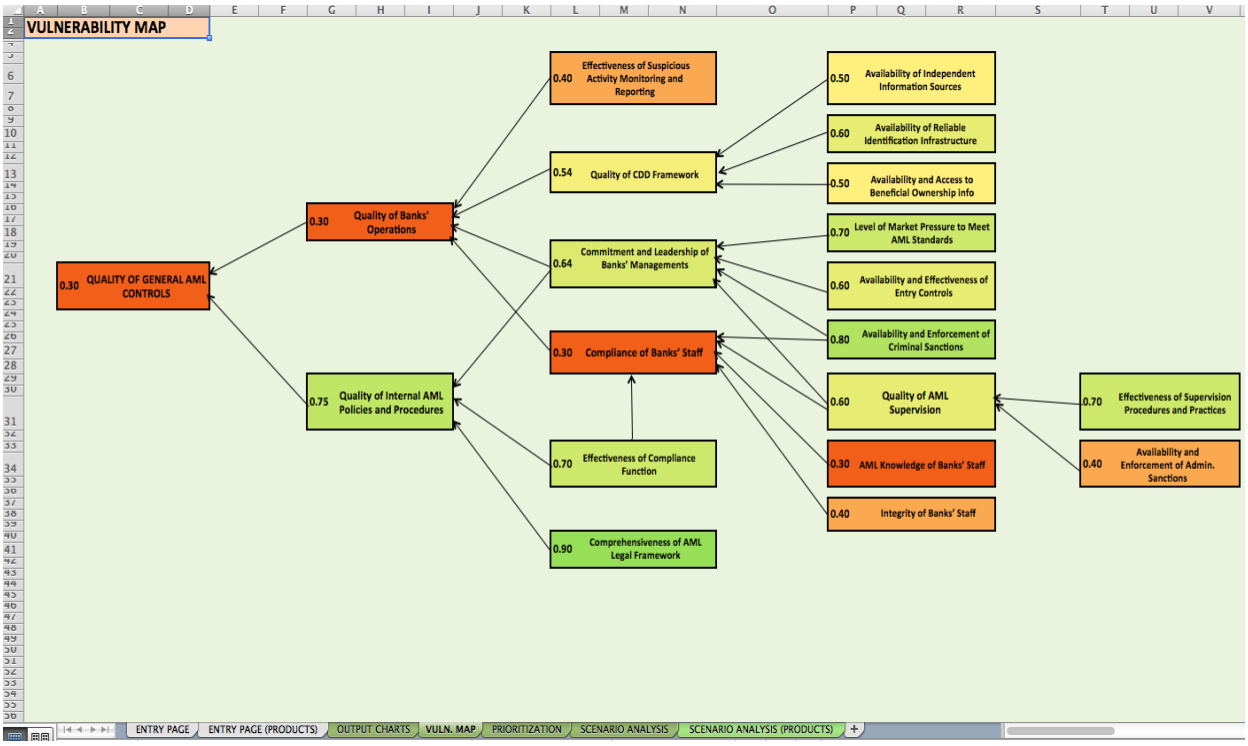
Please pay attention to the names and the colors of the inputs and outputs while interpreting the scores.

- 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, a high score 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 banking sector, click on the **Vulnerability Map** icon on the Entry Page (Products) tab (as shown in Figure 7). This tab provides a visual summary of the assessment ratings of all the variables (see Figure 9). 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 banking sector 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 banking sector.

Figure 9: Vulnerability Map



The assessment results in Figure 9 show that the quality of general 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 Internal AML Policies and Procedures* is good (this type of green indicates a medium-high score), the *Quality of Banks' Operations* is weak (the low score and the color red indicating weak operations). The problem area is therefore *Quality of Banks' Operations*. Low *Compliance of Banks' Staff* and weak *Effectiveness of Suspicious Activity Monitoring and Reporting Systems* in the banks underlie the deficiencies in bank operations. Furthermore, low *Integrity of Banks' Staff* and *AML Knowledge of Banks' Staff* are the factors underlying low *Compliance of Banks' Staff*.

3. *Prioritization tab*

A priority ranking can be generated to help guide relevant authorities to prioritize actions to strengthen AML controls within the banking sector. Click on the **Prioritization** icon in the Entry Page (Products) tab (Figure 7) or in the Output Charts tab (Figure 8) 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 sector vulnerability (see Figure 10).

Figure 10: Prioritization table

PRIORITY RANKING - LAST CASE/SCENARIO	PRIORITY RANKING**
Comprehensiveness of AML Legal Framework	
Effectiveness of Supervision Procedures and Practices	
Availability and Enforcement of Administrative Sanctions	2
Availability and Enforcement of Criminal Sanctions	
Availability and Effectiveness of Entry Controls	5
Integrity of Banks' Staff	4
AML Knowledge of Banks' Staff	1
Effectiveness of Compliance Function (Organization)	
Effectiveness of Suspicious Activity Monitoring and Reporting	3
Level of Market Pressure to Meet AML Standards	
Availability and Access to Beneficial Ownership Information	7
Availability of Reliable Identification Infrastructure	6
Availability of Independent Information Sources	8

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

- 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 the 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 10, the input variable *AML Knowledge of Banks' 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:

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

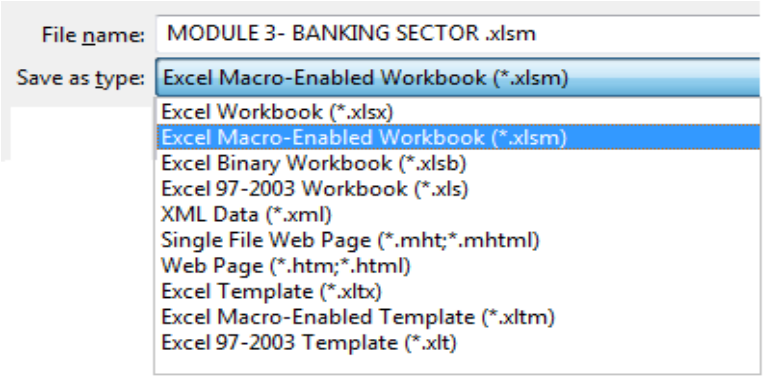
Whether an Open Door Approach or a Weighted Average Approach (or a combination of both) is used to assess the final vulnerability of the banking sector, all the outputs and assessment results discussed in Step 5 will be the same for all three approaches. Only the vulnerability of the banking sector, which is also a component of national vulnerability, 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 11). If it is not saved as a macro-enabled workbook, the macros will be disabled and the Excel file will not function properly.

Figure 11: Save Excel file as a macro-enabled workbook



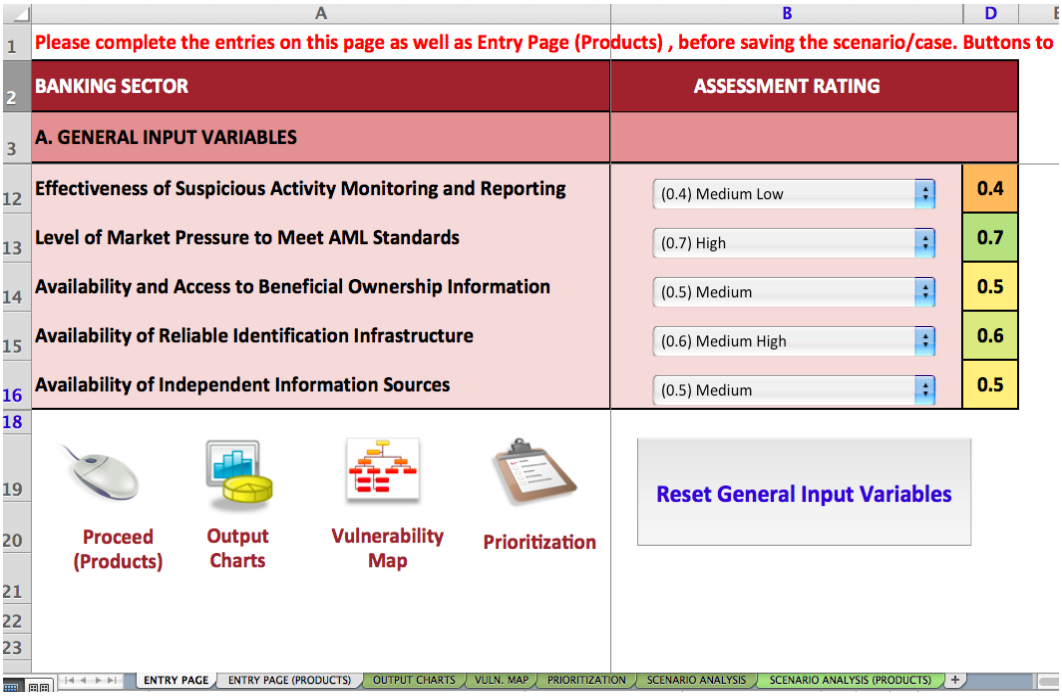
Changing entries after the original case has been saved

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 (Products) tab (see Figure 7). 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 Product Entries** icon on the Entry Page (Products) tab (Figure 7), and click the **Reset General Input Variables** icon on the Entry Page tab (Figure 12) to erase all the previous entries. Also click the **Clean Charts** icon on the Output Charts tab (Figure 8) to erase the previous entries on the Output Charts tab.

Figure 12: Icons on the Entry Page tab



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 banking sector 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, banking sector vulnerability, assessment results for intermediate variables, inherent variables, final product vulnerability, and priority ranking for the general input variables for different years or scenarios can all be compared using the scenario analysis option.

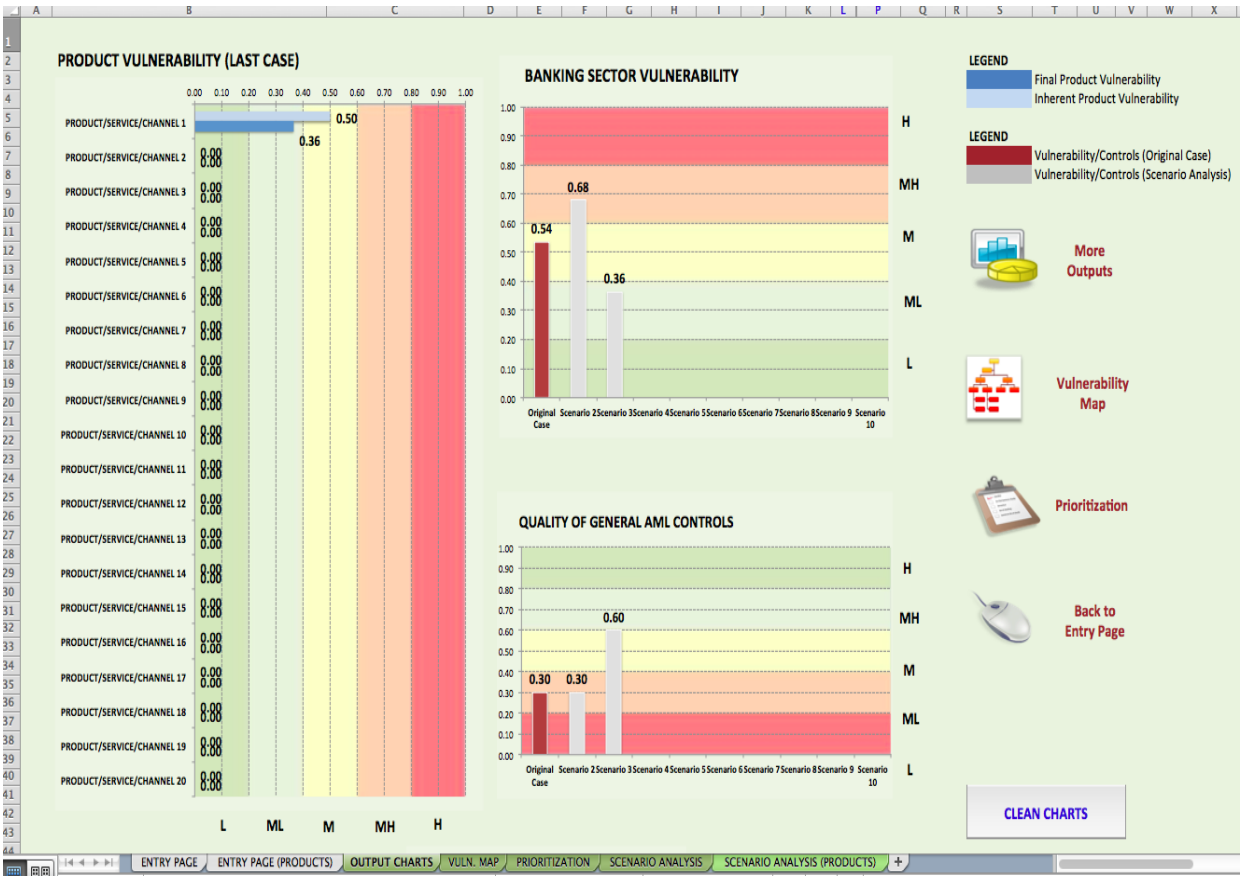
It is also possible to use the scenario analysis function for comparing the results of Open Door and Weighted Average Approaches.

Instructions for using the scenario analysis option

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/product-specific input variables for the second year, or for Scenario 2, in the Entry Page tab/Entry Page (Products) tab and save the entries as Scenario 2.

As in Step 5, assessment results are generated in the Output Charts tab (as shown in Figure 13). 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 13). Scenario analysis can be performed for 10 years, or for 10 different scenarios. In Figure 13, 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 banking sector vulnerability and the intermediate variables (such as *Quality of AML Controls* and *Quality of Banks' Operations*) are available for all the previous cases, as well as the last case (as shown in Figure 13).

Figure 13: Output charts – Scenario Analysis



Scenario Analysis results –– screen display

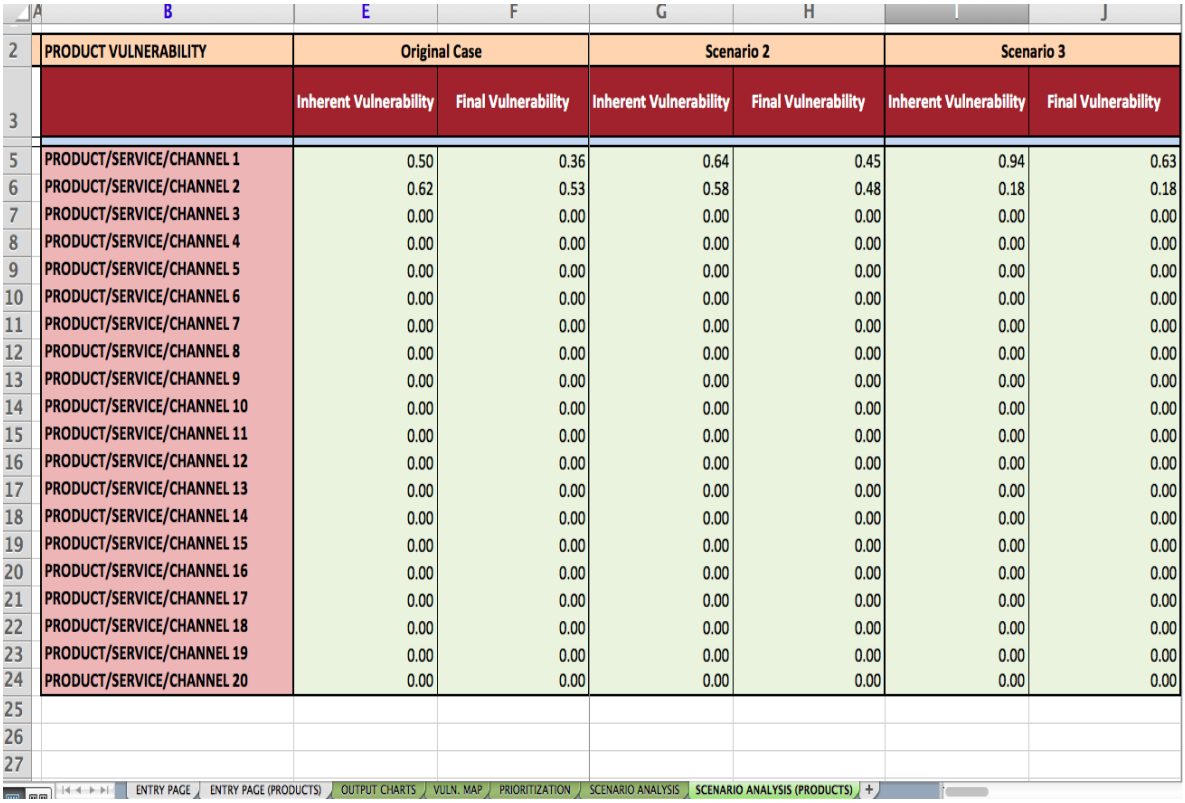
The Scenario Analysis tab and the Scenario Analysis (Products) tab provide the assessment results for the different years or scenarios (Figures 14 and 15). The Scenario Analysis tab shows the assigned assessment ratings for the general input variables, the assessment results for intermediate variables, the final banking sector vulnerability score, and the priority rankings of the general input variables for the various years/scenarios. The Scenario Analysis (Products) tab shows the inherent and final vulnerability for the products assessed for the various years/scenarios. These tables are helpful in understanding where changes in the vulnerability of the banking sector 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 14: Scenario Analysis tab

	A	C	D	E	F	G
1		Original Case	Scenario 2	Scenario 3	Scenario 4	Scenar
2	INPUTS/GENERAL INPUT VARIABLES					
3	Comprehensiveness of AML Legal Framework	0.9	0.9	0.9		
4	Effectiveness of Supervision Procedures and Practices	0.7	0.8	0.8		
5	Availability and Enforcement of Administrative Sanctions	0.4	0.5	0.6		
6	Availability and Enforcement of Criminal Sanctions	0.8	0.9	0.9		
7	Availability and Effectiveness of Entry Controls	0.6	0.6	0.6		
8	Integrity of Banks' Staff	0.4	0.7	0.7		
9	AML Knowledge of Banks' Staff	0.3	0.3	0.6		
10	Effectiveness of Compliance Function (Organization)	0.7	0.7	0.7		
11	Effectiveness of Suspicious Activity Monitoring and Reporting	0.4	0.4	0.7		
12	Level of Market Pressure to Meet AML Standards	0.7	0.5	0.5		
13	Availability and Access to Beneficial Ownership Information	0.5	0.5	0.5		
14	Availability of Reliable Identification Infrastructure	0.6	0.6	0.6		
15	Availability of Independent Information Sources	0.5	0.7	0.7		
16						
17	OUTPUTS/ASSESSMENT RESULTS FOR INTERMEDIATE VARIABLES					
18	BANKING SECTOR VULNERABILITY	0.54	0.68	0.36		
19	QUALITY OF GENERAL AML CONTROLS	0.30	0.30	0.60		
20	Quality of Banks' Operations	0.30	0.30	0.60		
21	Quality of Internal AML Policies and Procedures	0.75	0.75	0.76		
22	Quality of CDD Framework	0.54	0.57	0.57		
23	Compliance of Banks' Staff	0.30	0.30	0.60		
24	Quality of AML Supervision	0.60	0.70	0.73		
25	Commitment and Leadership of Banks' Managements	0.64	0.66	0.67		
26						
27	PRIORITY RANKING FOR GENERAL INPUT VARIABLES					
28	Comprehensiveness of AML Legal Framework					
29	Effectiveness of Supervision Procedures and Practices					
30	Availability and Enforcement of Administrative Sanctions	2	2	3		
31	Availability and Enforcement of Criminal Sanctions					
32	Availability and Effectiveness of Entry Controls	5	5	4		
33	Integrity of Banks' Staff	4				
34	AML Knowledge of Banks' Staff	1	1	1		
35	Effectiveness of Compliance Function (Organization)					
36	Effectiveness of Suspicious Activity Monitoring and Reporting	3	2			
37	Level of Market Pressure to Meet AML Standards		4	2		
38	Availability and Access to Beneficial Ownership Information	7	7	6		
39	Availability of Reliable Identification Infrastructure	6	6	5		
40	Availability of Independent Information Sources	8				

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

Figure 15: Scenario Analysis (Products) tab



PRODUCT VULNERABILITY	Original Case		Scenario 2		Scenario 3	
	Inherent Vulnerability	Final Vulnerability	Inherent Vulnerability	Final Vulnerability	Inherent Vulnerability	Final Vulnerability
PRODUCT/SERVICE/CHANNEL 1	0.50	0.36	0.64	0.45	0.94	0.63
PRODUCT/SERVICE/CHANNEL 2	0.62	0.53	0.58	0.48	0.18	0.18
PRODUCT/SERVICE/CHANNEL 3	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 4	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 5	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 6	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 7	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 8	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 9	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 10	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 11	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 12	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 13	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 14	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 15	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 16	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 17	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 18	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 19	0.00	0.00	0.00	0.00	0.00	0.00
PRODUCT/SERVICE/CHANNEL 20	0.00	0.00	0.00	0.00	0.00	0.00

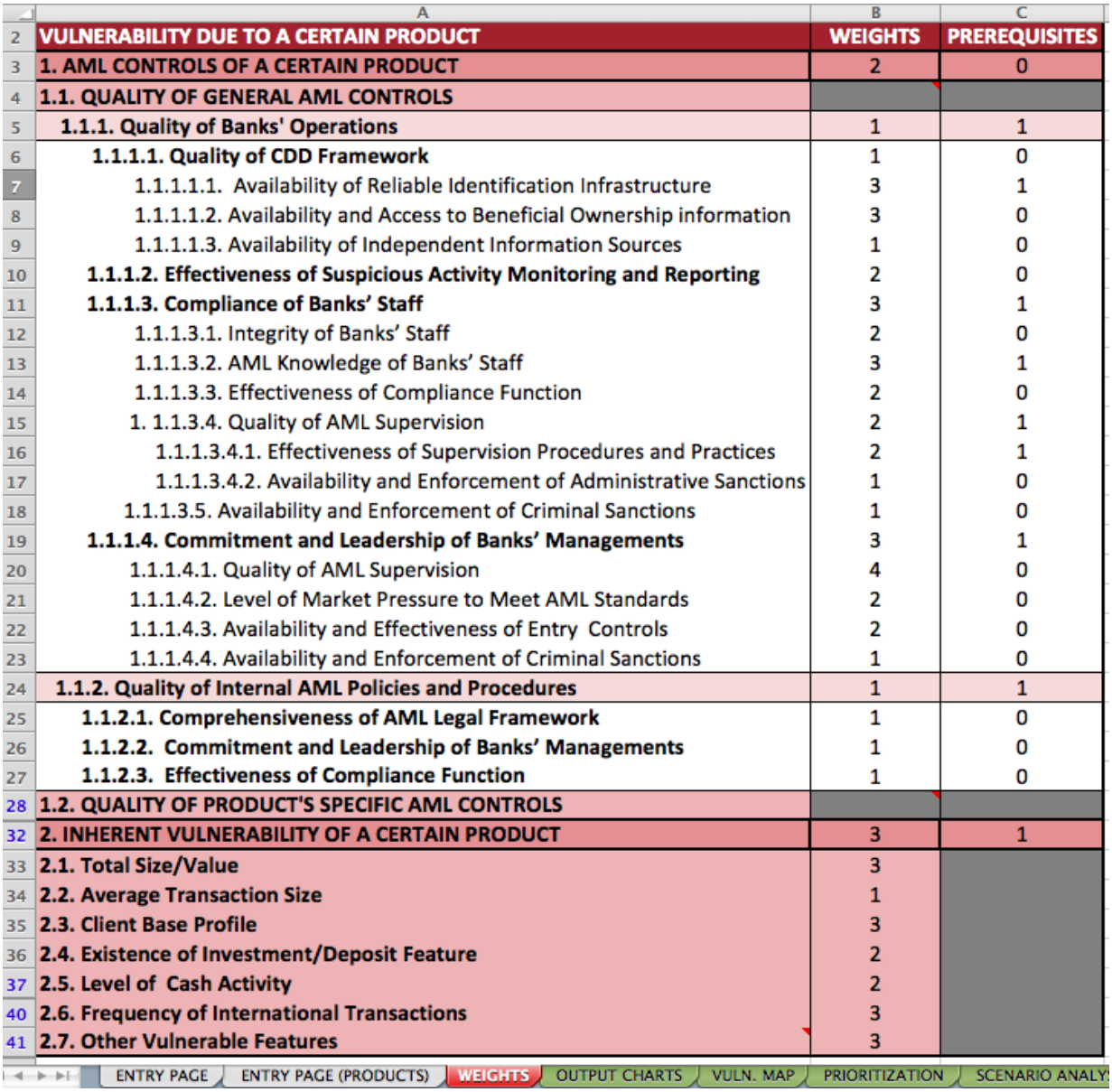
How to "unhide" the Weights tab

The default weights of the variables and pre-requisites of the intermediate variables reflect the assumptions that underlie the module. In the default version of the Excel file, the weights, the defined pre-requisites 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 pre-requisites are required.

In Figure 16, 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 Banks' Operations* (line 5) is determined by four variables:

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

Figure 16: Weights tab



	A	B	C
2	VULNERABILITY DUE TO A CERTAIN PRODUCT	WEIGHTS	PREREQUISITES
3	1. AML CONTROLS OF A CERTAIN PRODUCT	2	0
4	1.1. QUALITY OF GENERAL AML CONTROLS		
5	1.1.1. Quality of Banks' Operations	1	1
6	1.1.1.1. Quality of CDD Framework	1	0
7	1.1.1.1.1. Availability of Reliable Identification Infrastructure	3	1
8	1.1.1.1.2. Availability and Access to Beneficial Ownership information	3	0
9	1.1.1.1.3. Availability of Independent Information Sources	1	0
10	1.1.1.2. Effectiveness of Suspicious Activity Monitoring and Reporting	2	0
11	1.1.1.3. Compliance of Banks' Staff	3	1
12	1.1.1.3.1. Integrity of Banks' Staff	2	0
13	1.1.1.3.2. AML Knowledge of Banks' Staff	3	1
14	1.1.1.3.3. Effectiveness of Compliance Function	2	0
15	1. 1.1.3.4. Quality of AML Supervision	2	1
16	1.1.1.3.4.1. Effectiveness of Supervision Procedures and Practices	2	1
17	1.1.1.3.4.2. Availability and Enforcement of Administrative Sanctions	1	0
18	1.1.1.3.5. Availability and Enforcement of Criminal Sanctions	1	0
19	1.1.1.4. Commitment and Leadership of Banks' Managements	3	1
20	1.1.1.4.1. Quality of AML Supervision	4	0
21	1.1.1.4.2. Level of Market Pressure to Meet AML Standards	2	0
22	1.1.1.4.3. Availability and Effectiveness of Entry Controls	2	0
23	1.1.1.4.4. Availability and Enforcement of Criminal Sanctions	1	0
24	1.1.2. Quality of Internal AML Policies and Procedures	1	1
25	1.1.2.1. Comprehensiveness of AML Legal Framework	1	0
26	1.1.2.2. Commitment and Leadership of Banks' Managements	1	0
27	1.1.2.3. Effectiveness of Compliance Function	1	0
28	1.2. QUALITY OF PRODUCT'S SPECIFIC AML CONTROLS		
32	2. INHERENT VULNERABILITY OF A CERTAIN PRODUCT	3	1
33	2.1. Total Size/Value	3	
34	2.2. Average Transaction Size	1	
35	2.3. Client Base Profile	3	
36	2.4. Existence of Investment/Deposit Feature	2	
37	2.5. Level of Cash Activity	2	
40	2.6. Frequency of International Transactions	3	
41	2.7. Other Vulnerable Features	3	

ENTRY PAGE | ENTRY PAGE (PRODUCTS) | WEIGHTS | OUTPUT CHARTS | VULN. MAP | PRIORITIZATION | SCENARIO ANALY

The weights on these four variables in determining the *Quality of Banks' Operations* (line 5) are relative to one another, as follows. The weight of the variable *Compliance of Banks' Staff* (line 11) is three times that of the variable *Quality of CDD Framework* (line 6), while the variable *Quality of General AML Controls* (line 4) is determined equally by the variables *Quality of Banks' Operations* (line 5) and *Quality of Internal AML Policies and Procedures* (line 24) (both have an assigned weight of 1).

The defined pre-requisites for the intermediate variables are shown in Column C (see Figure 16). If a variable has a weight of 1 assigned to it in Column C, then it is a pre-requisite. For example, for the variable *Quality of CDD Framework* (line 6), the variable *Availability of Reliable Identification Infrastructure* (line 7) is a pre-requisite. 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.