WORLD BANK GROUP
Finance & Markets

NRA toolkit

NATIONAL RISK ASSESSMENT TOOL
GUIDANCE MANUAL

MODULE 4
SECURITIES 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 Securities Sector Vulnerability Module of the National ML/TF Risk Assessment Tool was developed by a World Bank team that was led by Emiko Todoroki, and included Kuntay Celik, Louis de Koker, and Ameet Kaur. The module is based on the structure of the Banking Sector Module. The team thanks the staff and the management of the World Bank's Financial Market Stability and Integrity team for their significant contributions, which played key role in the evolution of the module into its current state.

CONTENTS

Important Reminders for the Working Group

- Base your assessments on group discussions to ensure the inclusion of a wide array of perspectives. All members of the Working Group should contribute to discussions and 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, clearly identify 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 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, which 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 SECURITIES SECTOR VULNERABILITY MODULE

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

- Identify the overall vulnerability of the securities sector
- Identify securities institution types that have high vulnerability
- Identify on a needs basis the products or services[1] offered by the securities institution types with high ML vulnerability (see Annex 2)
- Prioritize action plans that will strengthen anti-money laundering controls (AML controls) in the securities sector.

The outcome of the Securities 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

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

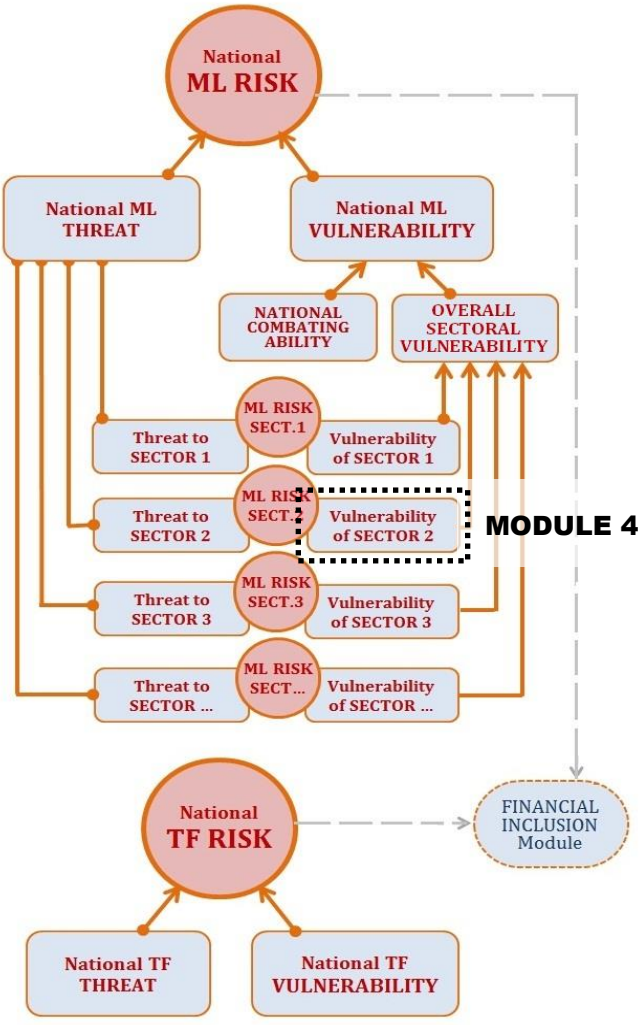
- Comparing the level of vulnerability of different types of securities institutions within the securities sector, and comparing the level of vulnerability in the securities sector with the vulnerability in other financial sectors
- Ensuring efficient resource allocation
- Developing specific AML controls for high-risk securities institution types/products.

2. UNDERSTANDING THE SECURITIES SECTOR VULNERABILITY MODULE

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

Figure 1: Securities 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 securities sector.

The levels of some AML control variables (such as *AML Knowledge of Staff* and *Staff Integrity*, etc.) may differ for various institutions types operating in the securities sector. For better analysis of the securities sector vulnerability, therefore, the assessment needs to be repeated for each type of institution operating within the securities sector.

Note that the module should be run separately for each of the identified types of securities institutions in a country.

Begin this exercise by making a list of the various types of securities institutions in your country.

Table 1: Proposed list of securities institution types

Below is a list of recommended types of securities institutions to provide a starting point for the Working Group. The Working Group is encouraged to modify the list depending on country context, as well as on the type of institutions present in the country.

- Independent securities broker-dealer (independent brokerage firms) – large
- Independent securities broker-dealer (independent brokerage firms) – medium/small
- Securities brokerage subsidiary of large commercial banks
- Securities brokerage subsidiary of medium/small commercial banks
- Large registered investment companies (mutual funds, closed-end funds, unit investment trusts, and private investment funds)
- Medium/small registered investment companies (mutual funds, closed-end funds, unit investment, trusts, and private investment funds)
- Large investment/financial advisors
- Medium/small investment/financial advisors
- Large wealth managers
- Medium/small wealth managers
- Net brokers (internet-based trading)
- Commodities futures and option broker – dealers, commodity trading advisors, futures commission merchant, futures pool operator – large
- Commodities futures and option broker – dealers, commodity trading advisors, futures commission merchant, futures pool operator – medium/small
- Unregistered investment companies (hedge funds, private equity funds, venture capital funds, commodity pools, and real estate investment trusts, REITS)

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

The Working Group (WG) can undertake a more detailed assessment of the products offered by each of the securities institution type. This should be decided on a needs basis, depending on the relevance of the securities institution type in question and the number of different products that may be offered by that type of institution. Assess different products in a particular institution type only if the products have different money laundering risks and there is benefit to be derived from detailed separate product analysis.

It is recommended that the assessment of the securities institution type be undertaken without a detailed product assessment.

The assessment for products is carried out in the same way as the assessment for the securities institution types. Note that the assessment criteria detailed in Section 4 also apply to the product-based assessment. For more details on the product-based assessment module, refer to Annex 2.

The WG should use Excel file 4.A if assessment is undertaken without detailed product assessment. In case of product-based assessment, use Excel file 4.B.

2.3. Variables

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

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

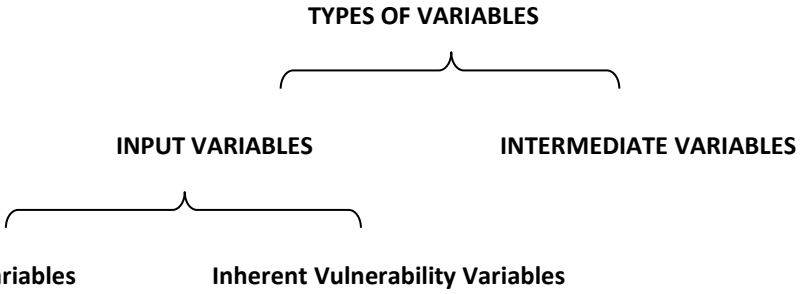
    a. ***AML control variables*** apply to the entire securities institution type, and should be assessed at the institution type level. This type of input variables relate to the quality and effectiveness of the AML controls, and therefore affects the vulnerability of the entire institution type being assessed.

    b. ***Inherent vulnerability variables*** relate to the specific features and users of a particular type of securities institution. An example would be a client base profile. As the client base profile for each institution type may vary, and consequently affect its vulnerability, it is necessary to assess the risks related to the client profile separately for each institution type.

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.

Figure 2: Variables in the Securities Sector Vulnerability Module

Securities Module (Default: Non-product-based assessment)



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

- Intermediate variables (pink boxes) do not require assessment.
- AML control variables (green boxes) need to be assessed for entire securities institution type.
- Inherent vulnerability variables (blue boxes) need to be assessed for each securities institution type.

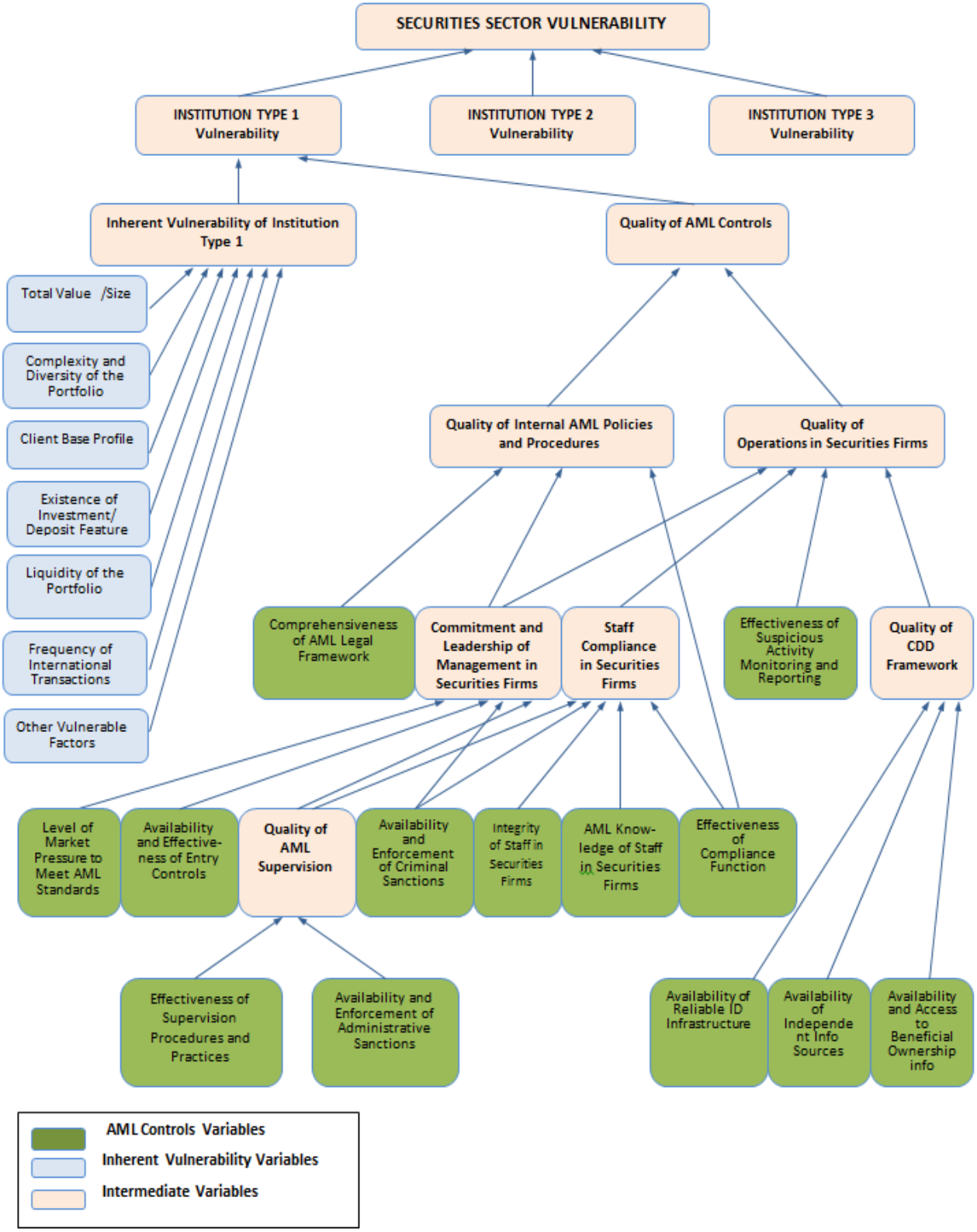
2.4. Module Structure (The Network)

The module is based on the assumption that the sector is similar to a building, with the different types of institutions being the various entrances to the building. Any money-laundering attempt needs to enter the securities 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 institution types operating in the sector will lead us to the overall vulnerability of the sector.

As illustrated in Figure 3.a, the overall vulnerability of the securities sector is determined by the vulnerabilities of the different institution types. Assessing the vulnerability of existing securities institution types, therefore, contributes to a comprehensive assessment of the vulnerability of the securities sector as a whole. This module assumes that the vulnerability of an institution type can be measured by two main factors, which are determined by underlying sub-factors: (1) inherent vulnerability (of the institution type) and (2) AML controls (of the institution type). "Institution Type 1" is used as an example in Figure 3.a. Similar assessments can be performed for other securities institution types.

Once the results for various institution types have been collated, the Working Group can begin to combine the results to obtain an overall vulnerability score for the securities sector. While combining these vulnerability scores, it is recommended that the Working Group use weighted averages. Weights may be decided either according to the institution type's share in the securities market or according to its vulnerability score.

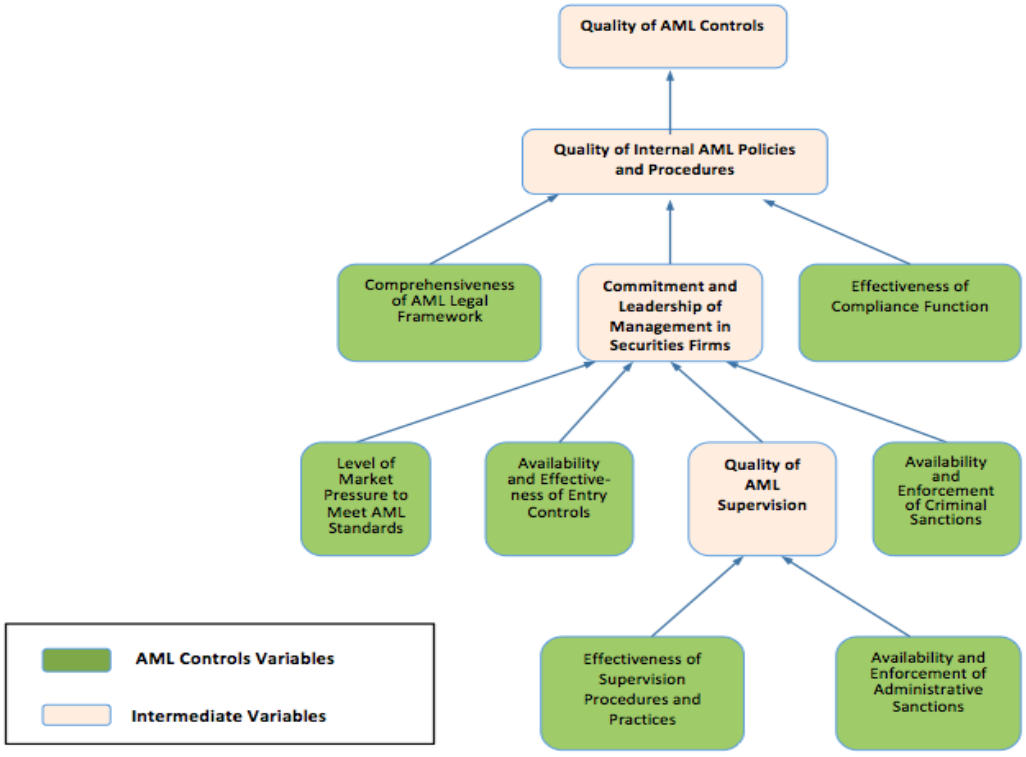
Figure 3.a: Securities Sector Vulnerability Module structure (Excel file 4.A)



2.5. The Logic behind the Network

In Figure 3.b, a small part of the structure is highlighted, in order to clarify the logic of the module. In particular, this refers to how the **input variables** and **intermediate variables** contribute to determining overall vulnerability. Please compare Figure 3.b with Figure 3.a to see how this segment fits into the whole network 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 assessed securities institution type affect the quality of AML controls. Clearly there is an impact, but not a direct impact.

The availability and enforcement of administrative sanctions increases the supervisory authority's ability to apply pressure on the managements of the securities firms. This supervisory pressure strengthens the commitment of securities firm managements to ensure AML compliance and to show leadership in the matter. As a result, the managements start to take action to improve the quality of the internal AML policies and procedures of their firms. Eventually, the securities firms begin to have better AML controls. As a result, the vulnerability of the securities institution type, as well as the overall securities sector 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 the *Quality of AML Supervision*, which is itself an intermediate variable. Input variables require direct input from the WG, while the intermediate variables do not – as illustrated in Figure 3.a (i.e., intermediate variables have arrows feeding into them, while input variables do not). For descriptions of intermediate variables, see Section 5.

Factors that determine the vulnerability of the securities institution type

There are four factors that determine the vulnerability of the securities *institution type*. These are:

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

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

The calculation

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

3. GENERAL GUIDANCE FOR THE ASSESSMENT

3.1. Introduction

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

The ratings of the input variables affect the vulnerability of the securities institution types in different directions.

- **AML controls.** Higher ratings reduce vulnerability of securities institution type, thereby decreasing vulnerability of the securities sector as a whole. Conversely, lower ratings increase the vulnerability of the securities institution type and the securities sector as a whole.

- **Inherent vulnerability variables.** Higher ratings increase the vulnerability of the institution type; thereby increasing the securities sector vulnerability, while lower ratings decrease the vulnerability of both the securities institution type and the securities sector.

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 supports 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 main stages:

> **Stage 1.** Assessing and rating the input variables, and supporting the assessment with data and information.
>
> **Stage 2.** Filling in the Excel file, and obtaining and interpreting the outputs.

Stage 1 is the most important and most time-consuming, and therefore calls for good time management. During the first workshop, preliminary ratings can be entered into 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 1 provides detailed instructions on how to use the Excel file (Stage 2). During the sessions in the first workshop, allocate most of your time to Stage 1, and save the final two hours for Stage 2.

Common input variables that appear in all modules

The input variables *Availability and Access to Beneficial Ownership Information*, *Availability of Reliable Identification Infrastructure*, and *Availability of Independent Information Sources* are included in every module of the tool, and are assessed at a national level. The assessment rating for these variables should be consistent across all modules, and should be based on systematic and logical reasoning. Unless there is sufficient rationale to assess these separately, the Securities Sector team can obtain the ratings for these variables from the National Vulnerability or Banking Sector teams.

3.3. Period for Information and Data Collection

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

Table 2: Guidance on information and data collection period

INDICATORS	INFORMATION AND DATA COLLECTION PERIOD
Quantitative indicators of vulnerabilities	Ten, five, or three years, depending on the availability of the data.
Qualitative indicators of vulnerabilities	Do not require a strict timeframe. The most meaningful information is the most recent information. Obtain as much information from the last five years as possible.

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

3.4. Possible Sources of Information and Data

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

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

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

4. ASSESSMENT WORKSHEETS FOR INPUT VARIABLES

4.1. Assessment Worksheets for General Input Variables

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

The AML control variables for this module relate to the strength of the AML controls. These variables affect the vulnerability of all institutions within the securities institution type. This assessment applies across the whole institution type and should therefore consider all the institutions operating within that institution type. Note that this assessment needs to be undertaken separately for each of the institution types assessed within the securities sector. The 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 Staff in Securities Firms*
7. *AML Knowledge of Staff in Securities Firms*
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 assessed securities institution type, 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, the vulnerability of the securities institution type is determined by the module. For example, therefore, the assessment should rate how effective the supervisory body is, not the impact of its effectiveness on the vulnerability of the assessed securities institution type. 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). This does not mean that the Mutual Evaluation Report (MER) findings are binding on the WG. The WG is encouraged to make use of many different reports and analyses that assess the ML risk of a country.

Recording the grounds of the assessment

Assessment worksheets for the module are given 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 *AML Controls* assessments should be filled out on the Entry Page tab in the Securities Sector Vulnerability Excel file. This should only be done after every variable has been assessed. Refer to Annex 1 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 for the securities institution type being assessed.

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

Assessment criteria

A country has comprehensive AML laws and regulations in force for the assessed institution type if these laws and regulations 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, where correspondent banking, new technologies, and wire transfers are involved
- Reliance on Customer Due Diligence by third parties (including introduced business)
- Suspicious Transaction Reporting (STR)
- Licensing
- Tipping-off and confidentiality
- Internal controls, foreign branches, and subsidiaries
- Regulation and supervision of financial institutions
- Supervisory powers.

Possible sources of information and data

- Relevant laws, regulations, and enforceable guidance related to the items above
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed).

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 securities institution type being assessed. 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

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

- Is clearly identified within the laws and regulations
- Has appropriate authority and mandate to conduct AML compliance supervision
- Carries out its supervisory activities within a comprehensive supervisory framework (including clear supervision policies, procedures, and manuals)
- Possesses a good understanding and appreciation of the ML risk within the institution type being assessed
- Has a sufficient number of trained staff
- Equips staff with the necessary skills and up-to-date knowledge for AML compliance examinations
- Has the necessary resources to ensure AML compliance (technical capacity, budget, tools, etc.)
- Carries out a comprehensive, risk-based supervisory program that consists of on-site/off-site components on both regularly scheduled cycles and periodic spot-checks (risk-based and as necessary)
- Reports and records the examination results in a systematic way and is able to effectively use these records for policy purposes
- Exercises moral suasion that has a significant impact on the management of securities firms, 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 securities firms actually inspected (on-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 representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed).

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 noncompliance with AML laws and regulations. Sanctions should be applicable not only to financial institutions (which includes securities firms), but also to their directors and senior managements. 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 securities firm, or individual members of management or staff, in cases of noncompliance with AML obligations. Consider the number of administrative actions that have been taken against securities firms and their staff (of the assessed securities institution type) over the past few years for noncompliance 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 management and staff behavior in securities firms (such as monetary penalties, administrative actions, removal of critical staff, and suspension/withdrawal of licenses).

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

- Most persons working in the assessed institution type 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 in the assessed institution type.

**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 on administrative sanctions
- Statistics (by type) of past administrative enforcement actions taken by relevant authorities
- Information on the steps taken (or not taken) by securities firms in the assessed institution type to remedy infractions
- Interviews/consultations with representatives from the institution type, including professional bodies and voluntary associations (which includes the forms of sanctions they enforce, such as disciplinary hearings or revocations of membership)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed).

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 noncompliance 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 (which include securities firms), but also to their directors and senior managements. 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 securities firm, or individual members of management or their staff (of the assessed securities institution type), in cases of noncompliance 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 assessed institution type 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 assessed institution type believe that criminal enforcement action would be initiated in the event of noncompliance with AML requirements.
- There is a record of convictions and criminal enforcement actions that have been taken over the past few years by law enforcement authorities regarding noncompliance with AML requirements in the assessed institution type. Consider the number of investigations, prosecutions, and convictions, as well as other available evidence on enforcement.
- Criminal enforcement against securities firms and their staff in the assessed institution type with regard to other financial crimes (such as fraud, etc.) may also give an insight into the perception of enforcement within the assessed institution type.

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 assessed institution type
- Statistics on criminal enforcement actions carried out by foreign law enforcement (and other relevant authorities) against firms and individual members of staff (of the assessed institution type), 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 representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities, law enforcement, and prosecuting agencies
- Surveys of management and staff from securities firms (of the institution type being assessed).

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 are comprehensive legal and regulatory frameworks, which provide authorities with appropriate powers, a sufficient level of staff, and other resources with which to carry out their duties. Effective entry controls help to reduce money-laundering vulnerability and to ensure 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 a good understanding and appreciation of ML risk in the assessed institution type
- Effectively carries out its licensing and entry controls duties
- Has a clear and comprehensive framework for the licensing and registration requirements of the assessed institution type including:
  - A fit and proper test designed to prevent criminals (or their associates) from being granted a license, having a significant controlling interest in a securities firm, or holding a significant management 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 securities firms, 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 representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed).

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 Staff in Securities Firms

Variable description

This variable assesses whether staff in securities firms act 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 staff members collude with criminals or undermine AML controls by acting corruptly, securities firms are vulnerable to money laundering abuse. Consider (1) the effectiveness of staff vetting programs within the assessed securities institution type, (2) the incidence of disciplinary action for breaches of integrity-related rules, and (3) the number of criminal cases taken against staff members.

Assessment criteria

Staff members in securities firms are regarded as acting with integrity if the following criteria are met:

- Securities firms 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 staff is low (but consider whether there is underreporting of incidences of integrity failure.
- There are appropriate mechanisms in place to protect securities firms' staff against any negative consequences resulting from reporting STR, or other actions that comply with AML obligations.

Possible sources of information and data

- Relevant laws/regulations (including specific provisions on confidentiality mechanisms in place for the staff when reporting suspicious or other relevant transactions)
- Information on staff vetting and training programs (of the assessed institution type)
- Interviews/consultations with representatives from the institution type, including professional bodies and voluntary associations (particularly internal control, or compliance units)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Findings of securities firms (of the assessed institution type) AML on-site/off-site examinations
- Statistics on integrity breaches by staff in securities firms in the assessed institution type and the disciplinary actions taken as a result
- Statistics on the number (and types) of administrative enforcement actions taken against firms and individuals working in the assessed institution type
- Statistics on criminal cases, including ML cases against staff in securities firms (of the assessed institution type)
- Review of reports/records of internal control/compliance units in securities firms (of the assessed institution type)
- Historical data of incidents/breaches by staff (kept for operational risk management purposes)
- General level of integrity, or the operating environment within a 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 Staff in Securities Firms

Variable description

This variable assesses how well the staff in securities firms (of the assessed securities institution type) knows and understands their AML duties and responsibilities.

Assessment criteria

The staff of a securities firms (of the assessed institution type) have the required AML knowledge if the following criteria are met:

- Appropriate AML training programs and materials are available for staff members.
- 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 firms conduct 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 firms, its products 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 representatives from the institution type, including professional bodies and voluntary associations (particularly internal control, or compliance units)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Findings of on-site/off-site AML examinations of securities firms (of the assessed institution type)
- Statistics and information on AML training activities by securities firms (hours of training, number of trainees, frequency of training, level and type of staff being trained, mandatory/voluntary participation, etc.)
- Information on AML training programs and training materials of securities firms (of the assessed institution type)
- Statistics on AML training given by public authorities to securities firms (of the assessed institution type).

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 securities firms of the assessed securities institution type have effective compliance function that is comprehensive, risk-based, and well resourced, with independent AML compliance function.

Assessment criteria

The assessed institution type possesses effective internal AML compliance function if most securities firms:

- Have internal compliance programs that are commensurate to the level of risk, taking into account factors such as the institution type, the volume and nature of the products provided, the client base profile, 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 for breaches of the 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 securities firms (of the assessed institution type)
- Findings from the AML on-site inspections and off-site monitoring
- Internal audit reports (and external, if any) on the adequacy and effectiveness of the compliance functions
- Statistics on any disciplinary actions taken by securities firms (of the assessed institution type) against their staff for breaches of the compliance policy
- Statistics on new clients, declined business, or terminated business relationships based on recommendations of the compliance staff
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed).

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 securities firms (of the assessed securities institution type) 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 securities firm with a single branch, but large securities firms 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

Securities firms (of the assessed institution type) have adequate and appropriate AML monitoring and STR systems if the following criteria are met:

- Securities firms have information systems that enable and facilitate the monitoring of client transactions against their profiles.
- Transactional records are available in a format that facilitates AML screening and monitoring.
- The systems support securities firms in performing effective PEP screenings.
- The systems assist securities firms and their staff to effectively identify and record all complex, unusual large transactions.
- The systems assist securities firms and their 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 obligations
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Findings from AML on-site/off-site examinations of securities firms (of the institution type being assessed)
- Information on the quality and accessibility of transaction records from securities firms (of the assessed institution type)
- Findings from supervisions, especially about the effectiveness of STR systems in place at securities firms of the assessed institution type (e.g., how many securities firms are compliant, and how many are not compliant? How does this impact the overall effectiveness of the STR reporting system in the assessed institution type?)
- Statistics on the number and the quality of STRs filed by securities firms (of the assessed institution type), including the number of STRs filed "defensively" (after being alerted to suspicious activity, or investigation by authorities)
- Statistics on the number of STRs relating to monitoring lapses that originate from securities firms (of the assessed institution type)
- Statistics on the number of STRs by securities firms (of the assessed institution type) referred to law enforcement agencies
- Information on the quality of STRs and the STR systems of securities firms (of the assessed institution type)
- Any other statistics on the outputs of the AML monitoring systems (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 the managements of securities firms (of the assessed securities institution type) to have effective AML compliance function. It addresses the pressures that exist outside a country's legal and supervisory regimes; for instance, commercial pressure applied by commercial counterparts, such as banks and/or other securities firms.

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

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

Assessment criteria

There is market pressure on managements in securities firms (of the assessed institution type) to meet international AML standards if the following criteria are met:

- They 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.
- Securities firms' managements are sensitive to international and national AML-related reputational risks.

Possible sources of information and data

- Interviews/consultations with representatives from the institution type (both within the country and any relevant external counterparts)
- Interviews/consultations with supervisory authorities type (both within the country and any relevant external counterparts)
- Surveys of management and staff from securities firms (of the institution type being assessed).

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.

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

Possible sources of information and data

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

Assessment

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

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

4.1.12. Availability of a Reliable Identification Infrastructure

Variable description

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

Assessment criteria

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

The infrastructure may consist of:

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

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

Possible sources of information and data

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

Assessment

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

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

4.1.13. 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.

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

Possible sources of information and data

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

Assessment

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

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

4.2. Assessment Worksheets for the Inherent Vulnerability Variables

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

Note: Assessing each securities institution type with product-specific input variables is also an option (product-based assessment). The criteria for product-specific input variable assessments are the same as the criteria for assessing broader inherent vulnerability factors for the specific institution type. For a more detailed, product-based assessment, see Annex 2.

This section provides guidance for seven inherent vulnerability variables.

Inherent vulnerability factors

The following input variables reflect the inherent vulnerability factors.

1. *Total value/size of the institution type*
2. *Complexity and diversity of the portfolio of the institution type*
3. *Client base profile of the institution type*
4. *Existence of investment/deposit feature for the institution type*
5. *Liquidity of the portfolio of the institution type*
6. *Frequency of international transactions associated with the institution type*
7. *Other vulnerable factors of the institution type*

These seven inherent vulnerability input variables determine the vulnerability of each type of securities institution. The assessment of these seven inputs should be performed for each institution type separately. Therefore, if a country is assessing 10 securities institution types, (7*10=) 70 variables will need to be assessed.

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

The results of the inherent vulnerability variable assessments need to be entered into the **Entry Page (Vulnerability)** tab of the Securities Sector Vulnerability Excel file 4.A/4.B (Excel 4.B for product-based assessment) for each securities institution type that is being assessed. Please use separate Excel files for each securities institution type. This should only be done after all the variables have been assessed. For detailed instructions on how to use the Excel file, refer to Annex 1.

4.2.1. Total value/size of the institution type

Variable description

This variable assesses the total value/size of a particular institution type within the securities sector. The total value/size of a particular institution type in this sector is indicative of the level of ML vulnerability that may be introduced into the sector if associated risks are not mitigated. The objective of this indicator is to assess the importance of particular institution types within the securities sector, such as large wealth managers, in comparison to other institution types such as broker/dealers.

The larger the value and importance of the institution type, the easier it is for criminals to camouflage "dirty" transactions, and the more difficult it is for institutions to red-flag and detect these.

Assessment criteria

The most appropriate indicator of the total value/size of an institution type is the value of the assets under management. Other indicators are the total account value, total commission income, management fees, or other types of fees associated with the institution type being assessed.

The actual number of transactions and amounts involved may be difficult to determine. What is required is a judgment as to whether the total value of an institution type is significant within the sector or not.

Possible sources of information and data

- Data on total assets under management associated with the assessed institution type
- Data on total account value associated with the assessed institution type
- Data on total commission income/management fees/other types of fees associated with the assessed institution type
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Interviews with, and data compiled by, private sector research/consulting firms.

Additional guidance

During the assessment, supervisory agencies need to refer to the balance sheet/income statement/account balances of all the securities firms under an institution type. While assessing the total value/size of an institution type, decide whether it is significant or not. If it is significant, give it a high rating, if it is not significant; give it a low rating (if you think it is moderately significant, give it a medium rating).

4.2.2. Complexity and diversity of the portfolio of the institution type

Variable description

This variable assesses the diversity of the assessed institution type's investment portfolio, and the complexity of the instruments in this portfolio. Diverse portfolios with complex instruments increase the inherent vulnerability of the institution type, as these features can attract more sophisticated money launderers, and can provide them with more opportunities, as well as potentially making the transactions more difficult to red-flag and trace.

If the WG prefers to use a product-based assessment for a particular type of institution, it should ensure that this assessment is completed in terms of assessing the complexity of each product.

Assessment criteria

Consider the number, complexity, and diversity of the instruments/portfolio offered by the securities institution type being assessed. Compare the complexity and diversity of the portfolio of the assessed institution type with other institution types operating within the securities sector, as well as other financial institutions within your country.

If you are using a product-based assessment, compare the complexity of the products being offered with other institution types in the securities sector, as well as other financial institutions in your country.

While assessing diversity and complexity, focus your attention on the actual portfolio of the institution type, rather than on availability or possibility. This is necessary because (for example) although a variety of securities products may be available in the market, the actual market itself may be insignificant.

Possible sources of information and data

- Data on the activities and transactions of the assessed institution type
- Data on the portfolio and instruments offered by the assessed institution type
- Off-site/on-site examination reports (including prudential supervision)
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Interviews with, and data compiled by, private sector research or consulting firms.

4.2.3. Client base profile of the institution type

Variable description

This variable assesses whether the type of client using the assessed institution type increases the risk of money laundering abuse within the securities sector.

Assessment criteria

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

- Domestic/international Politically Exposed Persons (PEPs)
- High-net-worth individuals
- Non-resident clients (particularly from high-risk jurisdictions)
- Clients with foreign business or personal interests
- Multiple accounts, or nominee accounts, at a single securities dealer for no apparent reason
- Clients with criminal records, or past administrative and/or supervisory actions against them
- Clients with business links to known high-risk jurisdictions
- Clients gained through introduced business (particularly from unregulated professional intermediaries or regulated intermediaries in jurisdictions with low AML controls)
- Businesses with complex and non-transparent ownership structures.

Possible sources of information and data

- Regulatory framework for risk-based classification of customers
- Regulatory framework for identifying and monitoring PEPs
- Any product/institution type statistics on PEPs, or other high-risk customers
- Securities sector data by institution type on international wire transfers/transactions
- Securities sector data by institution type concerning transactions with high-risk jurisdictions
- Data on crime, including ML cases in which an institution type was used for ML purposes by high-risk customers
- Statistics on STRs originating from the assessed institution type with regard to high-risk customers
- Interviews/consultations with representatives from the institution type (including professional bodies and associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Interviews with, and data compiled by, private sector research or consulting firms.

Additional guidance

While assessing the client base profile for each institution type, assess whether the particular institution type is being used by the customers who pose a higher money laundering risk than "standard" customers. These high-risk customers include Politically Exposed Persons (PEPs), non-residents, high-net-worth individuals, and so on. It would be useful to look at the geographical breakdown of client transactions. Many firms categorize transactions with high-risk jurisdictions as high risk for the purpose of screening and monitoring transactions and to identify suspicious transactions. Transactions associated with high-risk jurisdictions are likely to be more vulnerable to money laundering. This is because it is likely that adequate AML controls are not in place, making it easier for criminals to move illicit funds to and from these jurisdictions into the global financial system. In order to assess this variable, a country should oblige financial institutions to put in place appropriate mechanisms to identify and monitor high-risk individuals (including PEPs). If such monitoring/analysis mechanisms are not in place, firms may not be able to provide any information.

In many countries, the resident status of securities firm customer is recorded during the process of establishing the business relationship. In this way, securities firms should be able to identify non-resident clients, and to determine which kinds of institution types they use. More advanced analysis – based on the countries such non-resident clients originate from – will provide further insight into the risk levels of various nationals.

In some cases, the institution type used for securities transactions will determine the client base profile. For example, the client base profile of large wealth managers would most likely be high-net-worth individuals. While assessing this indicator, question how likely it is that criminals will abuse this type of institution for securities transactions compared to others. If the level of possibility is high, the assessment rating for the client base profile for this institution type should be relatively high.

If a country does not have appropriate mechanisms to identify and monitor high-risk customers (including PEPs), this indicator will require appropriate judgment. Additionally, if there is no data to support the assessment, the WG needs to consider the worst-case scenario and make a conservative 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 institution type

Variable description

This variable assesses whether an institution type allows the investment/deposit of funds into a financial system, which consequently increases the risk of money laundering abuse within the securities sector.

Assessment criteria

An institution type is likely to be more vulnerable to money laundering if it allows the investment/depositing of funds into a country's financial system. The extent of vulnerability to ML abuse for a particular institution type (due to the availability of investment/deposit feature) depends on whether such feature has extensive or limited functionality. For some institution types (such as large wealth managers), the investment/deposit feature is prominent and has extensive functionality due to the large sum of funds involved. This makes them more vulnerable to money laundering abuse than other institution types. For example, small brokers, who have limited investment/deposit functionality due to the small amount of funds being deposited, are therefore less attractive for money laundering purposes.

The WG needs to analyze the availability of investment/deposit features for the various institution types. The more functional such a feature is within the institution type, the more vulnerable the institution is to ML.

In the securities industry, most of the institution types allow for the investment/deposit of funds into a financial system. Hence, the assessment rating for most of the institution types for this variable should be either "Available and Prominent" or "Available".

The rationale for assessing this variable within the securities sector is so that the ML vulnerability of institution types can be compared to other financial institutions (such as banking and insurance), where not all the products allow for the investment/depositing of funds into a financial system. Assessing this variable makes it easier to compare ML vulnerability across the financial sector institutions.

Possible sources of information and data

- Securities firm (of the assessed institution type) product manuals
- Criminal data, including ML cases in which an institution type was used for ML due to the availability of investment/deposit feature
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Interviews with, and data compiled by, private sector research or consulting firms.

4.2.5. Liquidity of the portfolio of the institution type

Variable description

This variable assesses the liquidity of the investment portfolio of the assessed institution type (or in a product-based assessment, the liquidity of the assessed product). Liquid instruments are more attractive for money launderers, as liquidity allows them to enter and exit the sector rapidly. In addition, instruments that are more liquid may expedite the layering process, compared to those that are less liquid.

Assessment criteria

Consider the composition of the portfolio of the institution type being assessed, and pay attention to the liquidity of the major instruments within the portfolio. During this assessment, compare the liquidity of the portfolio of the assessed institution type with other institution types operating within the securities sector, as well as other financial institutions in your country.

If you are using a product-based assessment, compare the liquidity with the products being offered by other institution types in securities sector, as well as other financial institutions in your country.

Possible sources of information and data

- Data on the activities and transactions of the assessed institution type
- Data on the portfolio and instruments offered by the assessed institution type
- Off-site/on-site examination reports (including prudential supervisions)
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Interviews with, and data compiled by, private sector research or consulting firms.

4.2.6. Frequency of international transactions associated with the institution type

Variable description

This variable assesses the frequency of international transactions associated with the institution type, which could increase the risk of money laundering abuse (for that particular institution type).

Assessment criteria

If the assessed institution type involves international transactions, it may be vulnerable to ML. The higher the number of international transactions for an institution type, the more vulnerable that type of institution is to ML.

In some jurisdictions, a securities account can be used in lieu of a depository account in order to wire funds internationally. Money launderers can use securities accounts to wire illicit assets out of a jurisdiction.

Possible sources of information and data

- Securities sector data on international transactions (organized by institution types)
- Number of STRs filed in respect to these institution types
- Criminal data, including ML cases in which an institution type was used for ML and involved international transactions
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Interviews with, and data compiled by, private sector research or consulting firms.

Additional guidance

The objective of this indicator is to distinguish the vulnerabilities of the different institution types, based on the frequency of international transactions that occur over the course of delivery to a client.

Securities sector data on international transactions relating to various institution types should preferably be on a consolidated basis, and should take into account data from all the securities firms for the institution type. If possible, this analysis should cover data from the last full year (to take seasonal fluctuations into account), and all the branches of the securities firms for the assessed institution type. If that is not possible, the analysis may be limited to one (or a couple) of branches that are representative of all the branches for the assessed institution type, and may cover a shorter period of time (such as one month).

4.2.7. Other vulnerable factors of the institution type

Variable description

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

Assessment criteria

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

- Possible anonymous/omnibus use of the product in the institution type
- ML typologies on the abuse of the institution type
- Significant use of the institution type in market manipulation, insider trading, and securities fraud
- Tracing the transaction records of the institution type is difficult
- Significant non-face-to-face use of the product in the institution type
- Level of cash activity associated with the type of securities institution.

Possible sources of information and data

- Criminal data (including ML cases in which an institution type was used for ML) indicating vulnerability due to the above-mentioned factors
- Data on statistical and qualitative information from MLA, and formal or informal information/intelligence sharing requests from supervisory authorities, law enforcement, FIU, the tax authorities, and other relevant authorities
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Interviews with, and data compiled by, private sector research or consulting firms.

Additional guidance

Note that the existence of one or more of these factors may render an institution type vulnerable to money laundering.

Anonymous/omnibus use of the product in the institution type:
Assess whether anonymous use of the product is possible for the institution type. Also consider whether the beneficial owner(s) of the transaction is always identified. Does the institution type allow for omnibus use (i.e., where an investor known to the securities firm uses the product on behalf of several investors, or a pool of investors, who are unknown to the securities firm)? Omnibus transactions are vulnerable to money laundering, as the beneficial owner(s) of the funds involved in the transaction is/are not known. The security firms execute the transaction on behalf of others. The real owners are unknown and therefore not subject to Customer Due Diligence procedures.

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

Use of the institution type in market manipulation, insider trading, or securities fraud:
Assess the use of the institution type in market manipulation (e.g., “pump and dump” schemes), insider trading, or securities fraud (e.g., confidence/boiler room/Ponzi schemes). The ML risks posed by institution type in the securities industry are two-fold. First, these institution types are often used to generate illicit assets through market manipulation, insider trading, and fraud. Money launderers either use existing shares that are already publicly traded, or start a shell company for the express purpose of engaging in these illicit activities. Secondly, criminal organizations have been known to use illicit assets generated outside the securities industry to engage in market manipulation, insider trading, and fraud. The illicit assets that are generated are laundered through the securities industry itself or through other parts of the financial sector. The most common example of laundering would be the simple transfer of illicit proceeds to a bank account.

Separate reporting requirements for insider trading, market manipulation, and securities fraud might mean that ML STRs are not being submitted to the FIU in some jurisdictions. In such cases, consider the number of convictions, cases, and other evidence available that involves securities institutions in market manipulation, insider trading, and securities fraud.

Difficulty in tracing the transaction records of the institution type:
Assess whether transactions executed over the course of delivery of a product by an institution type have been properly recorded, and whether access to those records can be readily obtained. The difficulty in tracing records depends on the quality of the AML record-keeping systems of the securities firms. In some institution types it is much easier to trace records like large securities firms while for others like small financial advisors it may be more difficult to get records because of the difference in the quality of systems in place to meet AML requirements.

Non-face-to-face use of the product of the institution type:
Availability of non-face-to-face initiation of business relationships (with respect to a product of the assessed institution type) raises ML vulnerability. Even in the case of OTC derivatives, where non-face-to-face initiation of a product are not allowed, but non-face-to-face use of the product is, there is a possibility of ML vulnerability. But when non-face-to-face use is allowed, the vulnerability of the product may be lower, depending on the quality of CDD done during the face-to-face product initiation, and the existence of other controls that limit the use of the product by persons other than the account holder. These controls need to be assessed under the specific AML controls of that particular product, as discussed in Annex 2.

Level of cash activity associated with the institution type:
Assess whether the institution type allows for the use of cash, which could consequently increase the risk of money laundering abuse in that institution type, and within the securities sector. For example, the use of cash as a payment method for securities transactions makes the institution type being assessed more vulnerable to money laundering.

In certain countries, some depository institutions and securities intermediaries permit the use of cash for the purchase of securities products that can be used to introduce illicit funds into the securities industry, as well as to integrate and layer the illicit assets through securities trading and redemptions.

The WG needs to analyze the use of cash in the institution type within the securities sector. The more the institution type is cash-based, the more vulnerable it is to ML.

Summary of the assessment of the securities institution type:

Considering the assessment criteria and guidance, assess the inherent vulnerability variables associated with the securities institution type. For each institution type, check (✓) the appropriate option in the table. Repeat this for each institution type being assessed. The list of institution types may be amended as needed.

		Institution Type (Module 4.A) Product 1 (Module 4.B)	Product 2 (Module 4.B)	Product 3 (Module 4.B)	Product 4 (Module 4.B)	Product 5 (Module 4.B)
Total value/size	High					
	Medium High					
	Medium					
	Medium Low					
	Low					
	Not Analyzed					
Complexity and diversity of the portfolio	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					
Liquidity of the portfolio	High					
	Medium High					
	Medium					
	Medium Low					
	Low					
	Not Analyzed					
Frequency of international transactions	High					
	Medium High					
	Medium					
	Medium Low					
	Low					
	Does Not Exist					
	Not Analyzed					
	Available					

Summary of the assessment of the securities institution type:

Considering the assessment criteria and guidance, assess the inherent vulnerability variables associated with the securities institution type. For each institution type, check (✓) the appropriate option in the table. Repeat this for each institution type being assessed. The list of institution types may be amended as needed.

			Institution Type (Module 4.A) Product 1 (Module 4.B)	Product 2 (Module 4.B)	Product 3 (Module 4.B)	Product 4 (Module 4.B)	Product 5 (Module 4.B)
Other vulnerable factors	Anonymous/ omnibus use	Not Available					
	Existence of ML typologies	Exist and Significant					
		Exist					
		Exist but Limited					
		Does Not Exist					
	Use in market manipulation	Exist and 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 use	Available and Prominent					
		Available					
		Available but Limited					
		Not Available					
	Level of cash activity	High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Not Analyzed					
		Does Not Exist					

In the case of product-based assessment for securities institution types, assess the inherent vulnerability variables associated with each product in the assessed institution type. Repeat the assessment for all the assessed institution types. For more details, refer to Annex 2.

5. DESCRIPTION OF THE INTERMEDIATE VARIABLES

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

VARIABLE	DESCRIPTION
Quality of AML Supervision	This variable assesses whether the assessed securities institution type 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 Management in Securities Firms	This variable assesses the managements of securities firms' (of the assessed securities institution type) commitment and leadership in AML, and how the managements are influenced by the following variables: • *Availability and Effectiveness of Entry Controls* • *Quality of AML Supervision* (intermediate variable) • *Availability and Enforcement of Criminal Sanctions* • *Level of Market Pressure to Meet AML Standards (optional).*
Quality of Internal AML Policies and Procedures	This variable assesses the quality of internal AML policies and compliance procedures of securities firms in the assessed securities institution type, which depends on the: • *Comprehensiveness of AML Legal Framework* • *Commitment and Leadership of Management in Securities Firms* (intermediate variable) • *Effectiveness of Compliance Function (Organization).*
Staff Compliance in Securities Firms	This variable assesses the compliance level of staff in securities firms (of the assessed securities institution type) 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 (Organization)* • *Integrity of Staff in Securities Firms* • *AML Knowledge of Staff in Securities Firms.*
Quality of CDD Framework	This variable assesses whether a 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 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 Operations in Securities Firms	This variable assesses the quality of operations at securities firms in preventing money-laundering abuse within the assessed securities institution type. This variable depends on the: • *Commitment and Leadership of Management in Securities Firms* (intermediate variable) • *Staff Compliance in Securities Firms* (intermediate variable) • *Effectiveness of Suspicious Activity Monitoring and Reporting* • *Quality of CDD Framework* (intermediate variable).
Quality of AML Controls	This variable assesses the quality of AML controls within the assessed securities institution type (which are the standard AML controls applied to all the securities firms). This variable depends on the:

VARIABLE	DESCRIPTION
	• *Quality of Internal AML Policies and Procedures* (intermediate variable) • *Quality of Operations in Securities Firms* (intermediate variable).
Quality of Specific AML Controls (for a Product) (applicable for product-based assessment only)	This variable assesses the effectiveness of the specific AML controls, which are enhanced controls designed specifically for the product. They are considered effective when they prevent and detect money-laundering activities relating to a certain product (of the assessed securities institution type). This variable depends on the: • *Availability of Product-Specific AML Controls* • *Quality of Operations in Securities Firms* (intermediate variable) • *Quality of General AML Controls* (intermediate variable).
Product AML Controls (applicable for product-based assessment only)	This variable assesses the overall effectiveness of all the AML controls together for a product (of the assessed securities institution type) in preventing and detecting money-laundering activities. This variable depends on the: • *Quality of Specific AML Controls* (for a product) (intermediate variable) • *Quality of General AML Controls* (intermediate variable).
Inherent Vulnerability of the Assessed Securities Institution Type/ **Product Inherent Vulnerability (applicable for product-based assessment only)**	This variable assesses the susceptibility of a particular securities institution type/product to money laundering, based solely on the key inherent factors of the institution type/product without taking into account its AML controls. A securities institution type/product is inherently vulnerable when its characteristics render it open to money laundering abuse. This depends on inherent vulnerability variables, namely the: • *Total value/size of the institution type* (or product) • *Complexity and diversity of the portfolio of the institution type* (or product) • *Client base profile of the institution type* (or product) • *Existence of investment/deposit feature for the institution type* (or product) • *Liquidity of the portfolio of the institution type* (or product) • *Frequency of international transactions associated with the institution type* (or product) • *Other vulnerable factors of the institution type* (or product).
Securities Institution Type Vulnerability/ **Product Vulnerability (applicable for product-based assessment only)**	This variable assesses the overall susceptibility of a securities institution type/product to money laundering given its inherent vulnerability and the AML control mechanisms in place to address that vulnerability. The more susceptible an institution type/product is, the more money laundering transactions can occur undetected. This variable depends on the following: • *Inherent Vulnerability of the Securities Institution Type or Product* (intermediate variable) • *Product AML Controls/Quality of AML Controls* (intermediate variable). **The ratings of all the product vulnerability assessments (of the assessed securities institution type) determine the vulnerability of the assessed securities institution type. The ratings of all the assessed securities institution types' vulnerability assessments determine the vulnerability of the securities sector.**

ANNEX 1 – INSTRUCTIONS FOR USING THE EXCEL FILE

At this stage, the input variables have been assessed, and assigned a rating. These ratings now need to be entered into the Excel file.

The WG should use Excel file 4.A if assessment is undertaken without detailed product assessment. In case of product-based assessment, use Excel file 4.B. Note that the Excel file (4.A/4.B) should be run separately for each securities institution type in a country.

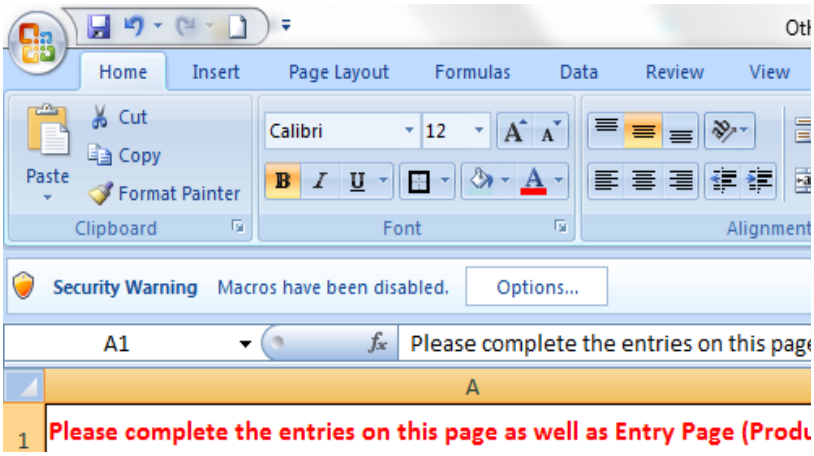
This Annex provides step-by-step instructions for using the Excel files 4.A/4.B to assess the vulnerability of the assessed securities institution type.

- 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

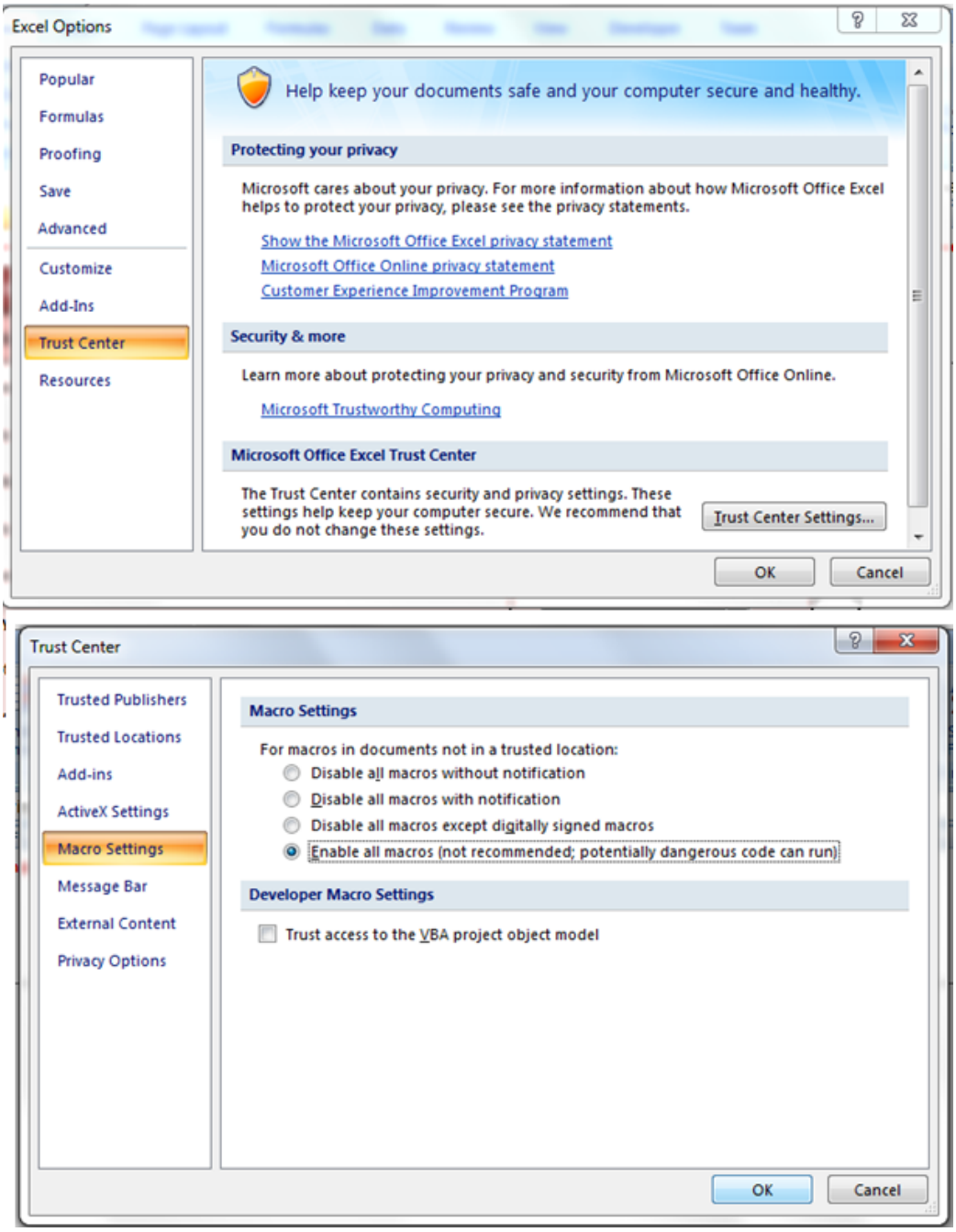
After opening the Excel file, first enable macros. A security warning will appear in the top left-hand corner of the first tab (Entry Page), warning you that macros are disabled – as shown in Figure 3. Click on the **Options** icon and select the **Enable this Content** option. Click **OK**, or (depending 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). When the Trust Center window opens, select the **Macro Settings** option (Figure 4.b). In this list, select the option **Enable all Macros** and click **OK**.

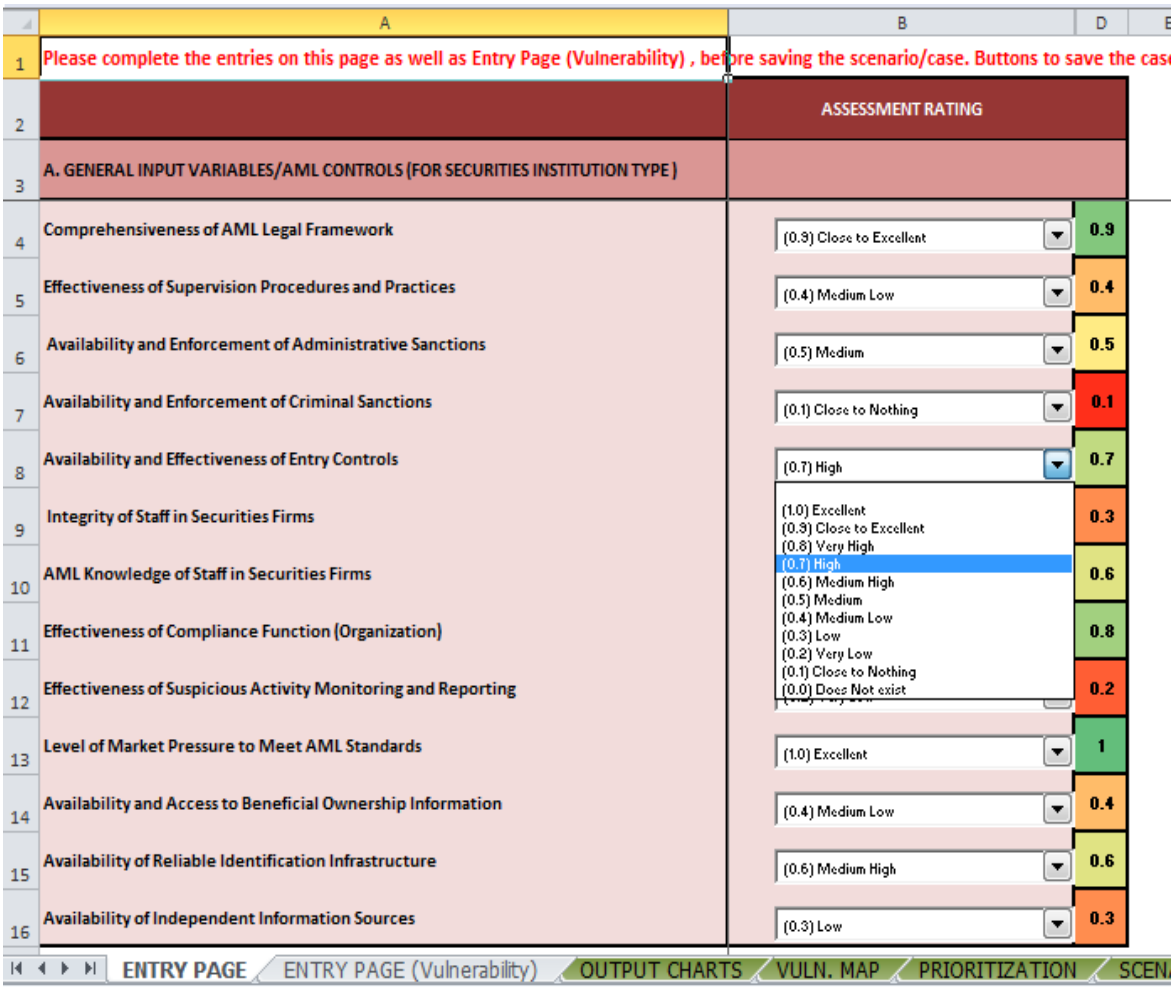
Figure 4.b: **Macro settings**



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

For each general input variable, select your chosen rating in the drop-down list. The options range from **(1.0) Excellent** to **(0.0) Does Not Exist**. Notice that higher assessment ratings for general input variables implies that the country has better AML controls in place, which will lead to a lower overall vulnerability for the assessed securities institution type. The Excel file automatically colors the entries according to their level of desirability (i.e., green=desirable, red=undesirable, etc.) – as shown in Figure 5. For both the Excel files (4.A and 4.B), the Entry (page) tab is similar.

Figure 5: **Entries for general input variables (in the Entry Page tab) – (Applicable to both Excel files 4.A and 4.B)**



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.

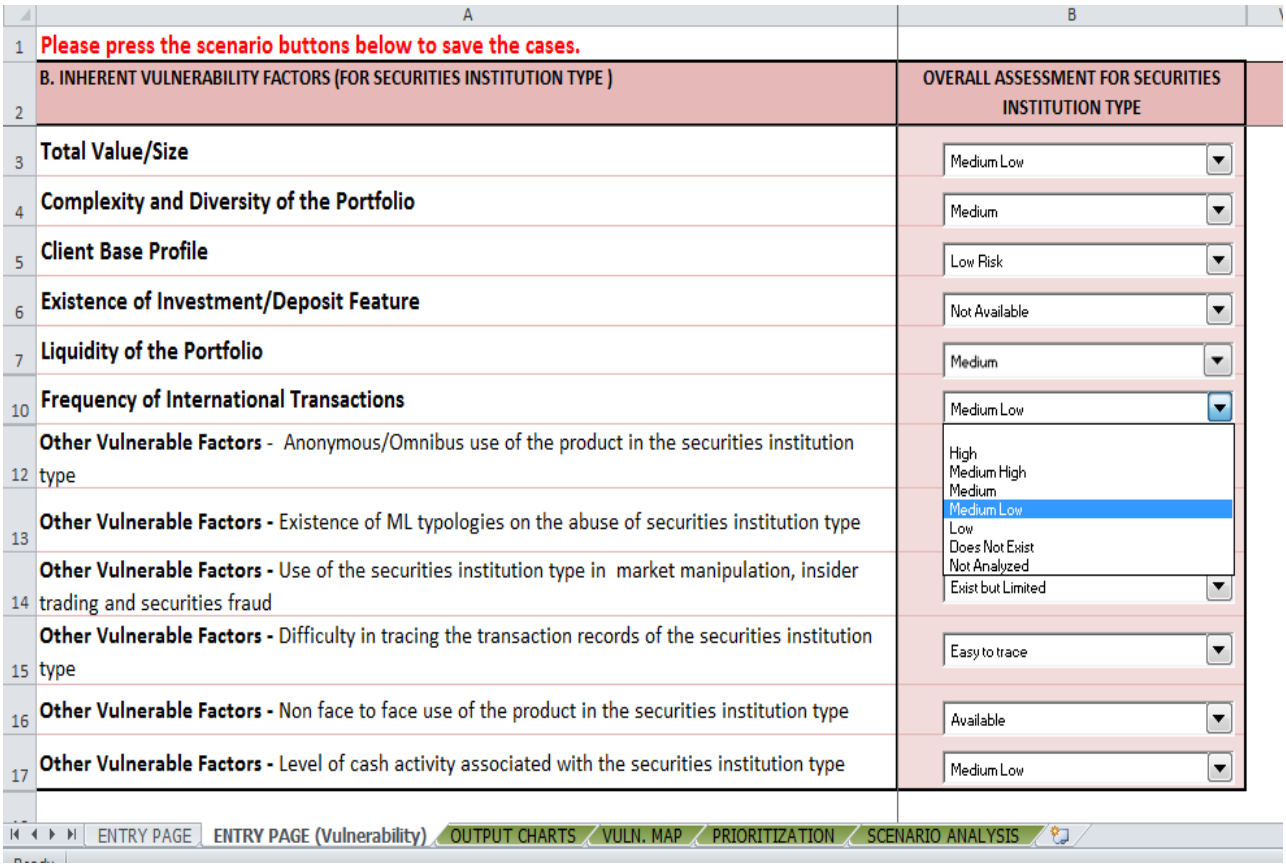
Bear in mind that the assessment of the general input variables is applicable to the whole institution type and should therefore consider all the firms operating within that institution type; and will influence the vulnerabilities of all the securities firms operating within the assessed institution type. In case of product-based assessment, it will also influence the vulnerabilities of all the products offered by the firms operating within the assessed institution type.

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

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

Enter the assessment ratings for each of the inherent vulnerability variables by clicking on the drop-down list in Column B (see Figure 6).

Figure 6: Entries for inherent vulnerability variables (in the Entry Page tab) – (Excel file 4.A)



If the rating for any inherent vulnerability variable has not been entered, a warning that the file is incomplete will appear in row 19 of the Entry Page (Vulnerability) tab.

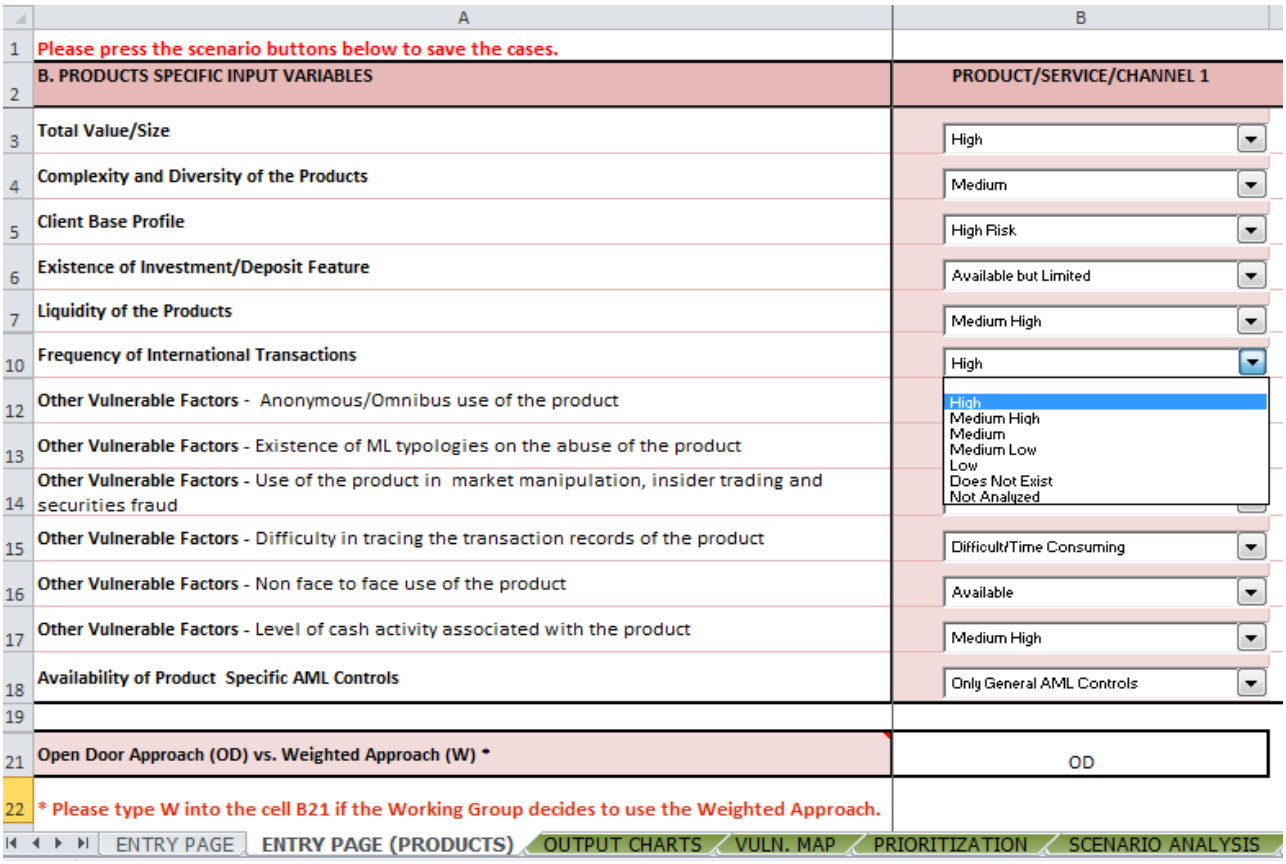
Step 3: Entries for inherent vulnerability variables and specific AML controls (in the Entry Page (Products) tab) (Applicable in case of product-based assessment – Excel file 4.B)

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

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

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 the vulnerability of the securities institution type, the Working Group 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 7: Entries for product-specific input variables (in the Entry Page (Products) tab) – (Excel file 4.B)



If the rating for any specific input variable has not been entered for a product, a warning that the file is incomplete will appear in row 19 of the Entry Page (Products) tab.

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

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

The Open Door Approach has been chosen as the default option in the Excel file 4.B. Thus, the entry in cell B 21 is "OD" (see Figure 7). If you prefer the Weighted Average Approach, switch to the weighted average option by entering "W" in this cell.

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

Step 4: Saving the entries

After the results for the input variables (step 2 and step 3) have been entered, save the entries by clicking the **Save the Original Case** icon on the Entry Page (Vulnerability) tab – as shown in Figure 8 or Entry Page (Products) tab – as shown in Figure 9 **(Applicable in case of product-based assessment – Excel file 4.B)**. This is an important step as the case needs to be saved before you can proceed. Otherwise, the output charts will not show the results of the assessment. (Bear in mind that this saves only your entries, not the file. You still have to save the Excel file to not lose your data.)

Figure 8: Icons on the Entry Page (Vulnerability) tab – (Excel file 4.A)

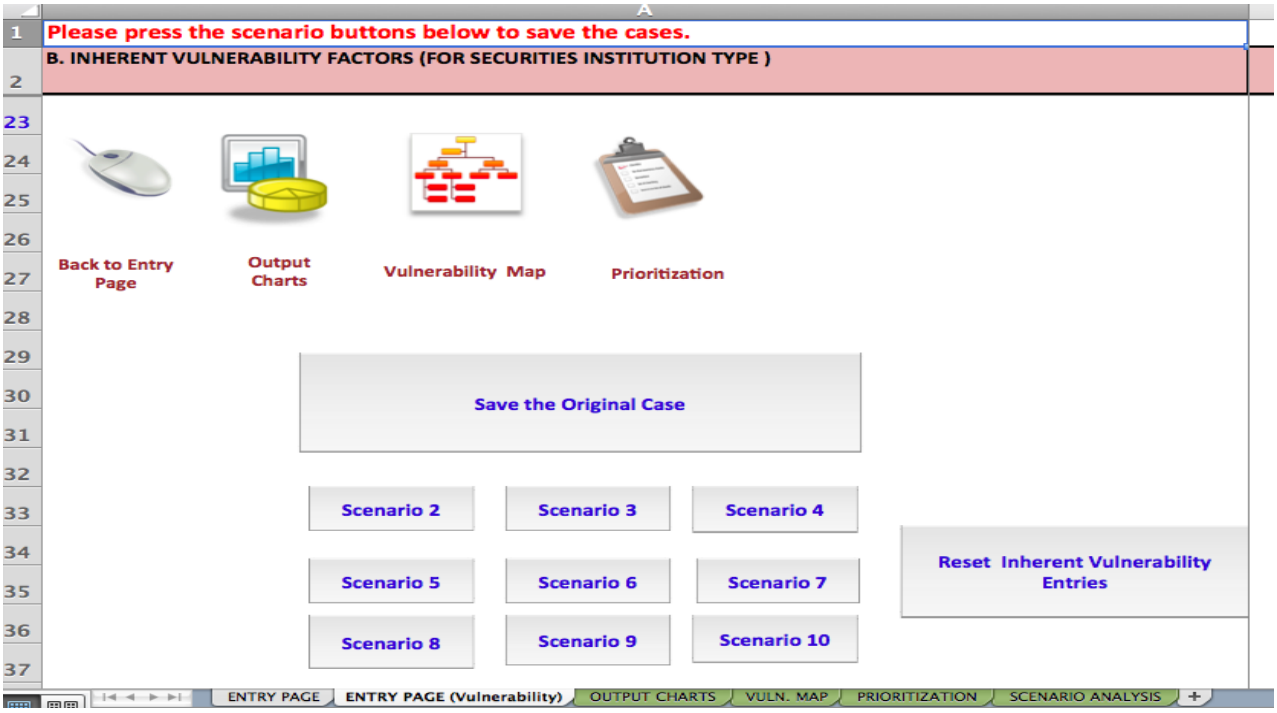
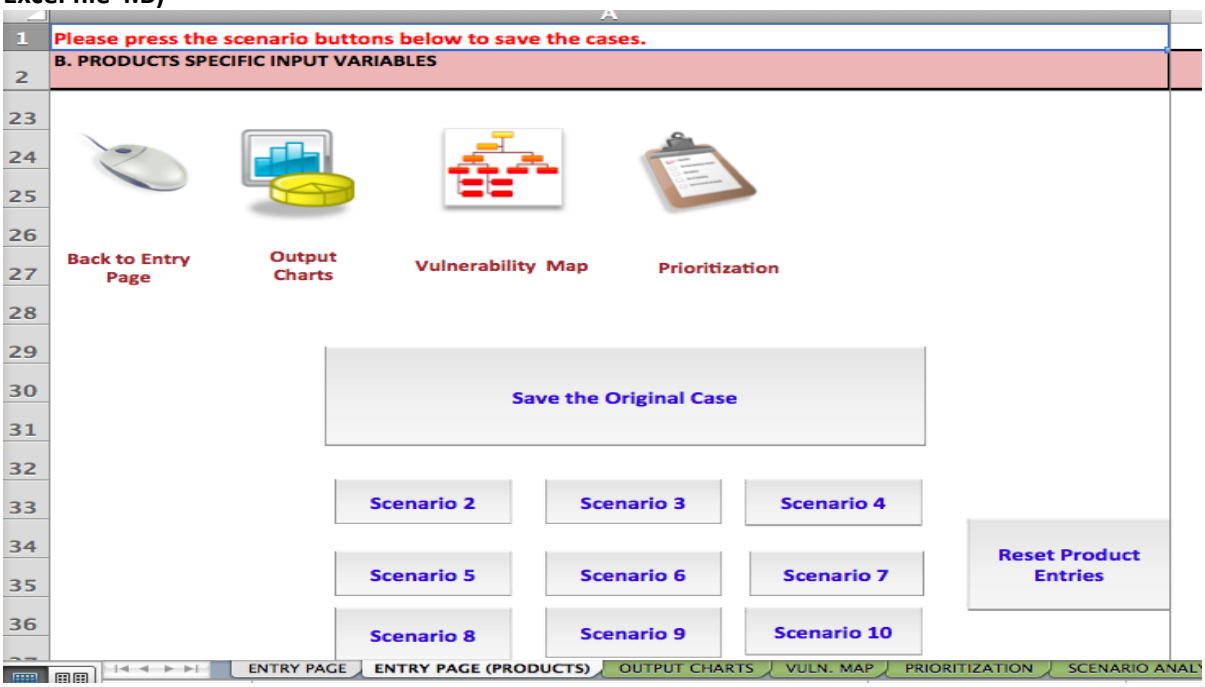


Figure 9: Icons on the Entry Page (Products) tab – (Applicable in case of product-based assessment – Excel file 4.B)



Step 5: The outputs of the assessment

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

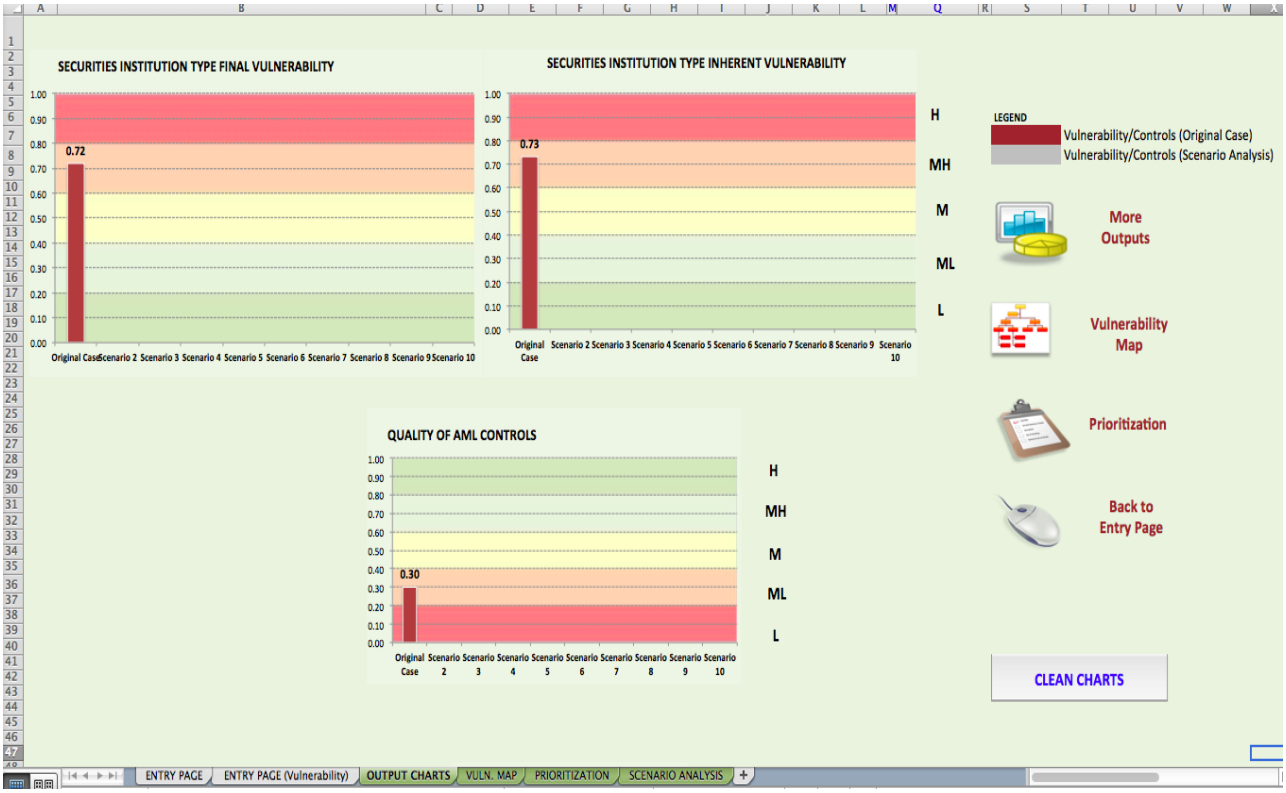
1. Output Charts
2. Vulnerability Map (Network Diagram)
3. Prioritization.

(1) Output Charts tab

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

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

Figure 10: Output charts (Excel file 4.A)



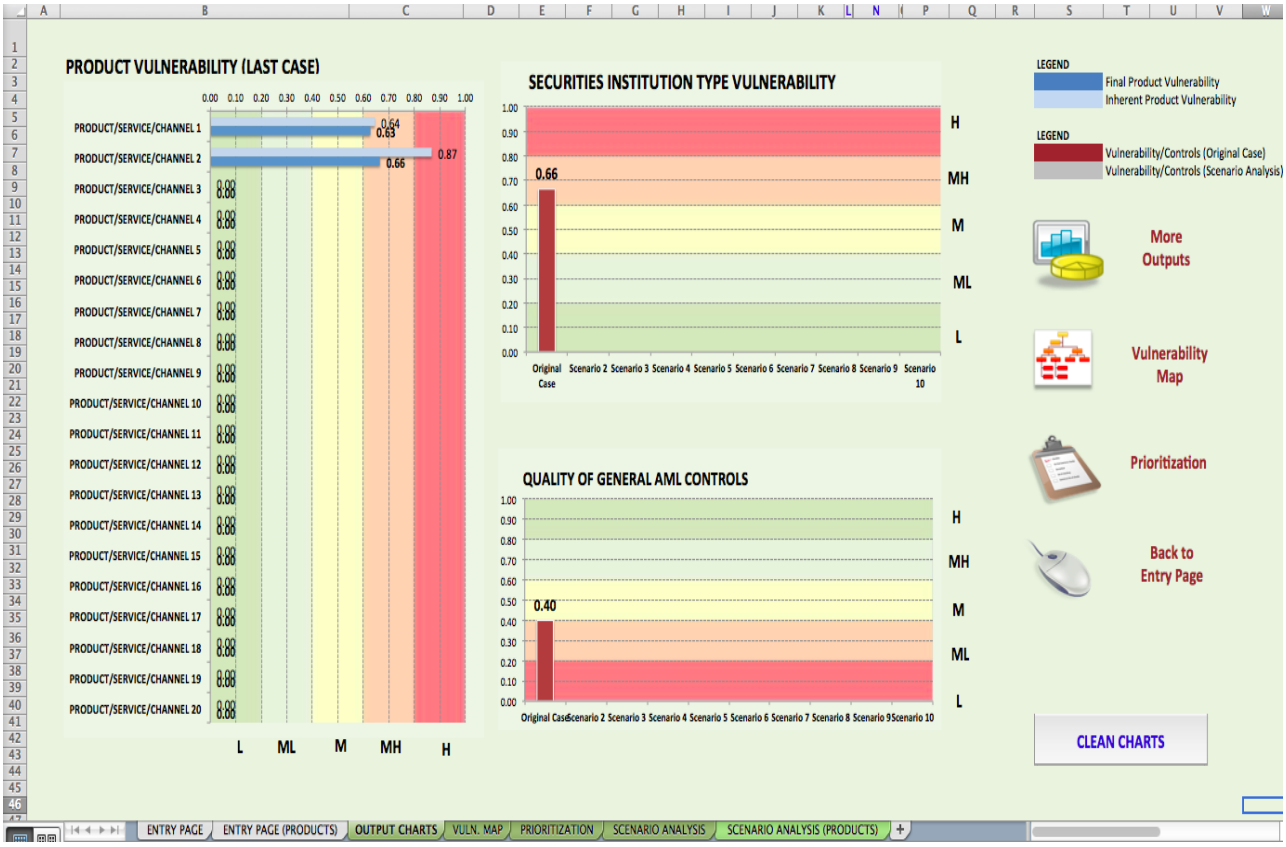
For both the vulnerability charts, a higher score implies a higher vulnerability to ML. On the other hand, for intermediate variables that relate to controls (such as *Quality of AML Controls, Quality of CDD Framework*, and *Staff Compliance in Securities Firms*) a higher score indicates a higher combating ability, which lowers the vulnerability of the assessed securities institution type to ML.

Output Charts tab – For product-based assessment (Excel file 4.B)

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

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

Figure 11: Output charts (Applicable in case of product-based assessment – Excel file 4.B)



For both the product vulnerability chart and the final vulnerability of the assessed securities institution type chart, a higher score implies a higher vulnerability to ML. Similarly, a higher product vulnerability score increases the vulnerability score of the assessed securities institution type.

On the other hand, for intermediate variables that relate to controls (such as *Quality of General AML Controls, Quality of CDD Framework*, and *Staff Compliance in Securities Firms*) a higher score indicates a higher combating ability, which lowers the vulnerability of the assessed securities institution type to ML.

Applicable to both the Excel files (4.A and 4.B)

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

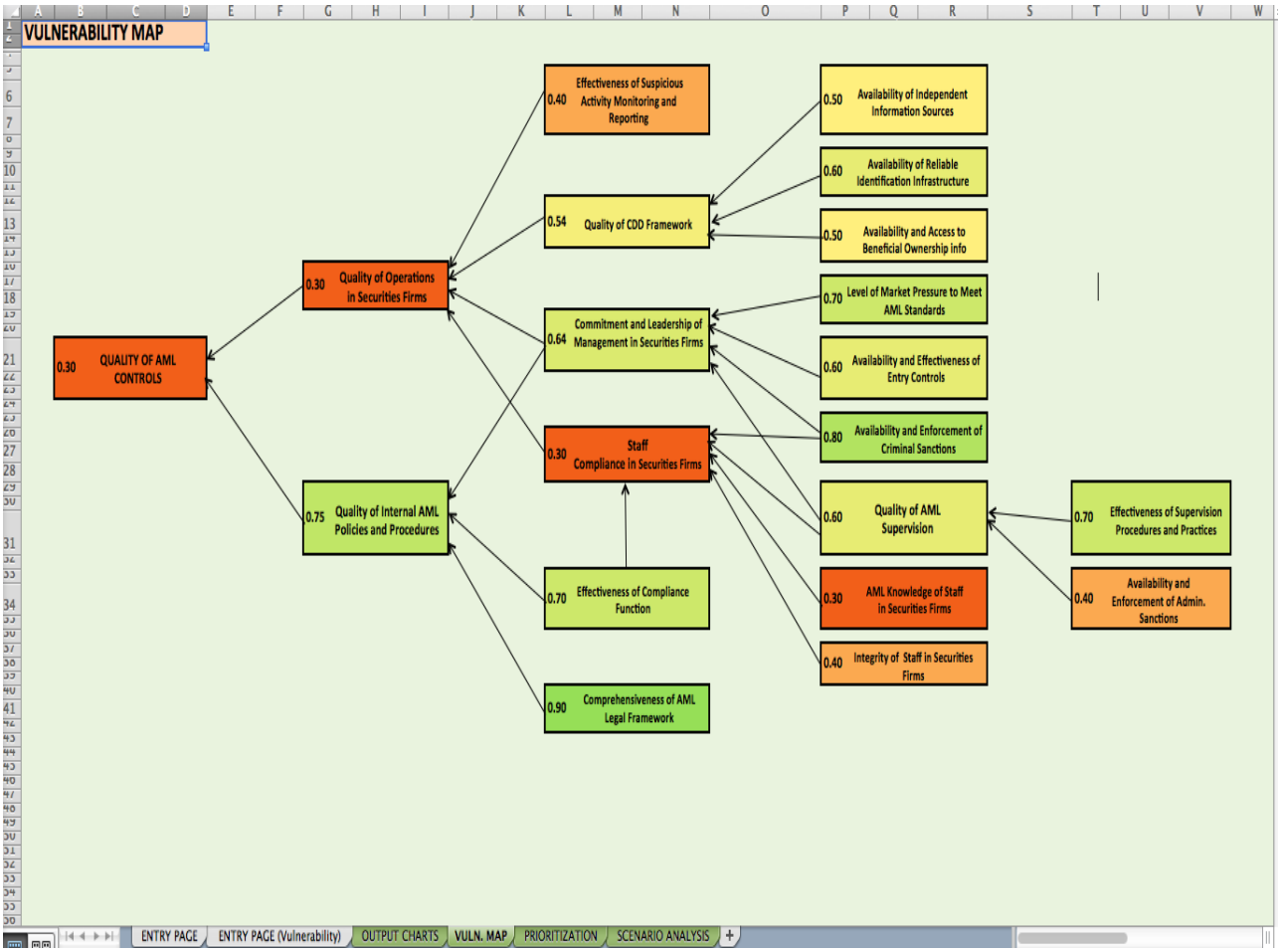
Please pay attention to the names and the colors of the inputs and outputs while interpreting the scores.

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

(2) Vulnerability Map tab

Vulnerability Map is a visual summary of the assessment, which shows how the assessment inputs cause impact on the outputs. To view the vulnerability map of the assessed securities institution type, click on the **Vulnerability Map** icon on the Entry Page (Vulnerability) tab (as shown in Figure 8) or Entry Page (Products) tab (as shown in Figure 9) for product-based assessment. This tab provides a visual summary of the assessment ratings of all the variables (see Figure 12). Note that the vulnerability map only shows the network diagram for the assigned assessment ratings of general input variables, and the corresponding assessment results of the intermediate variables, which affect the degree to which the assessed securities institution type is able to combat ML. This diagram does not show the effect of general input variables on product vulnerability, or the impact of product vulnerabilities on the final vulnerability of the assessed securities institution type (applicable only in case of product-based assessment – Excel file 4.B).

Figure 12: Vulnerability Map (Applicable to both the Excel files – 4.A and 4.B)



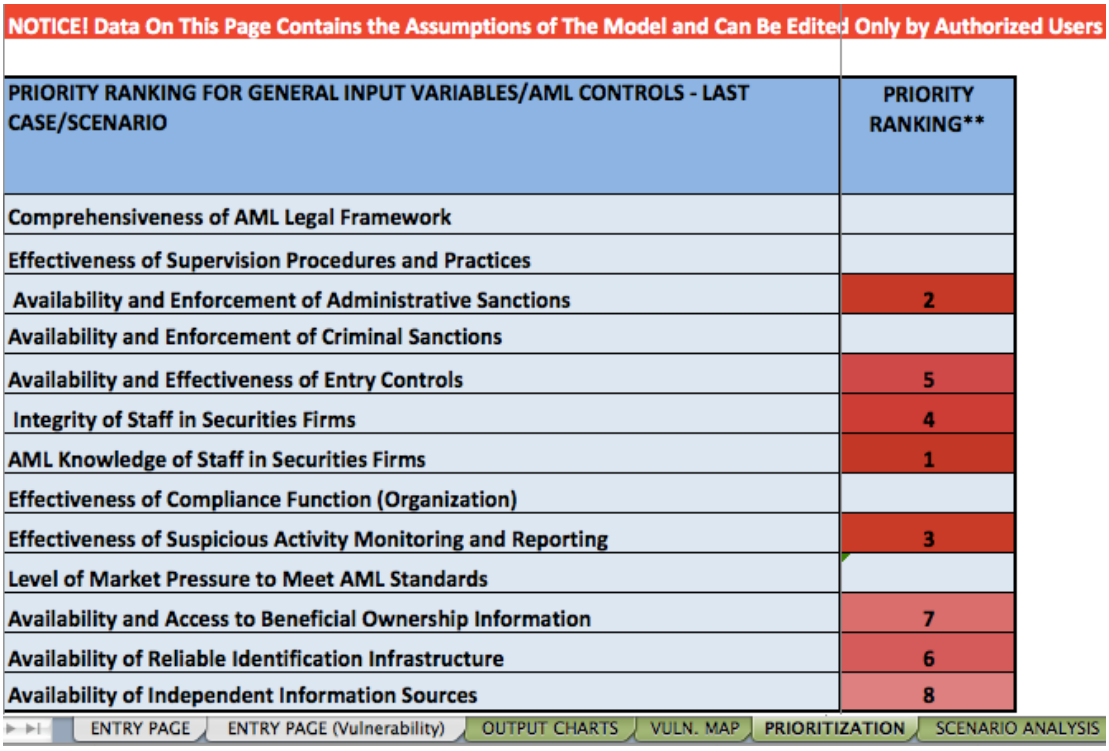
The assessment results in Figure 12 show that the quality of AML controls is weak. This can be seen in the low score and the red color of the box, both of which indicate weak AML controls. Although the *Quality of Internal AML Policies and Procedures* is good (this type of green indicates a medium-high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

(3) Prioritization tab

A priority ranking can be generated to help guide relevant authorities to prioritize actions to strengthen AML controls within the assessed securities institution type. Click on the **Prioritization** icon in the Entry Page (Vulnerability) tab (Figure 8) or in the Output Charts tab (Figure 10) to go to the Prioritization tab. In case of product-based assessment (Excel file 4.B), Click on the **Prioritization** icon in the Entry Page

(Products) tab (Figure 9) or in the Output Charts tab (Figure 11) to go to the Prioritization tab. The table in the Prioritization tab ranks the general input variables with respect to their impact on the AML controls and consequently the vulnerability of the assessed securities institution type (see Figure 13).

Figure 13: Prioritization table (Applicable to both the Excel files – 4.A and 4.B)



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

PRIORITY RANKING FOR GENERAL INPUT VARIABLES/AML CONTROLS - 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 Staff in Securities Firms	4
AML Knowledge of Staff in Securities Firms	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 (Vulnerability) | OUTPUT CHARTS | VULN. MAP | PRIORITIZATION | SCENARIO ANALYSIS

- 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 on the priority list, although it has less priority than the ones with darker colors.
- Blank cell (in light blue) indicates that the corresponding input variable does not have priority. There may still be deficiencies related to variable, but these are not severe and do not require urgent action.

For example, in Figure 13, the input variable *AML Knowledge of Staff in Securities Firms* 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.

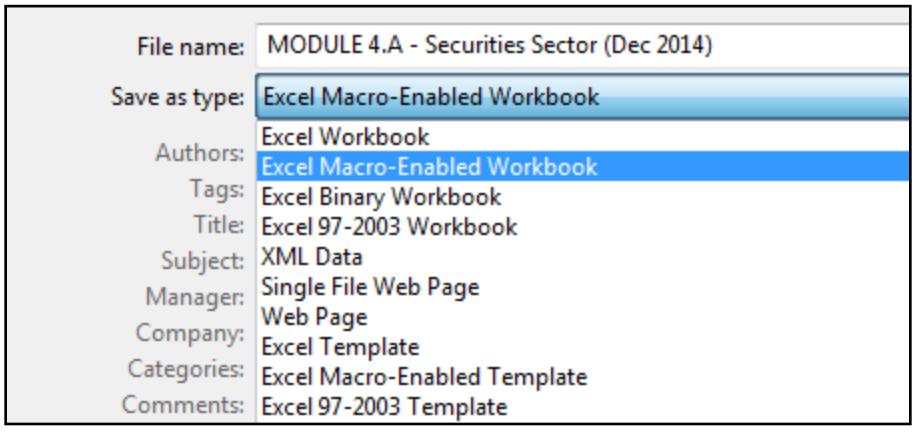
Applicable to product-based assessment – (Excel file 4.B)

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

Step 6: Saving the file

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

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



Changing entries after the original case has been saved

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

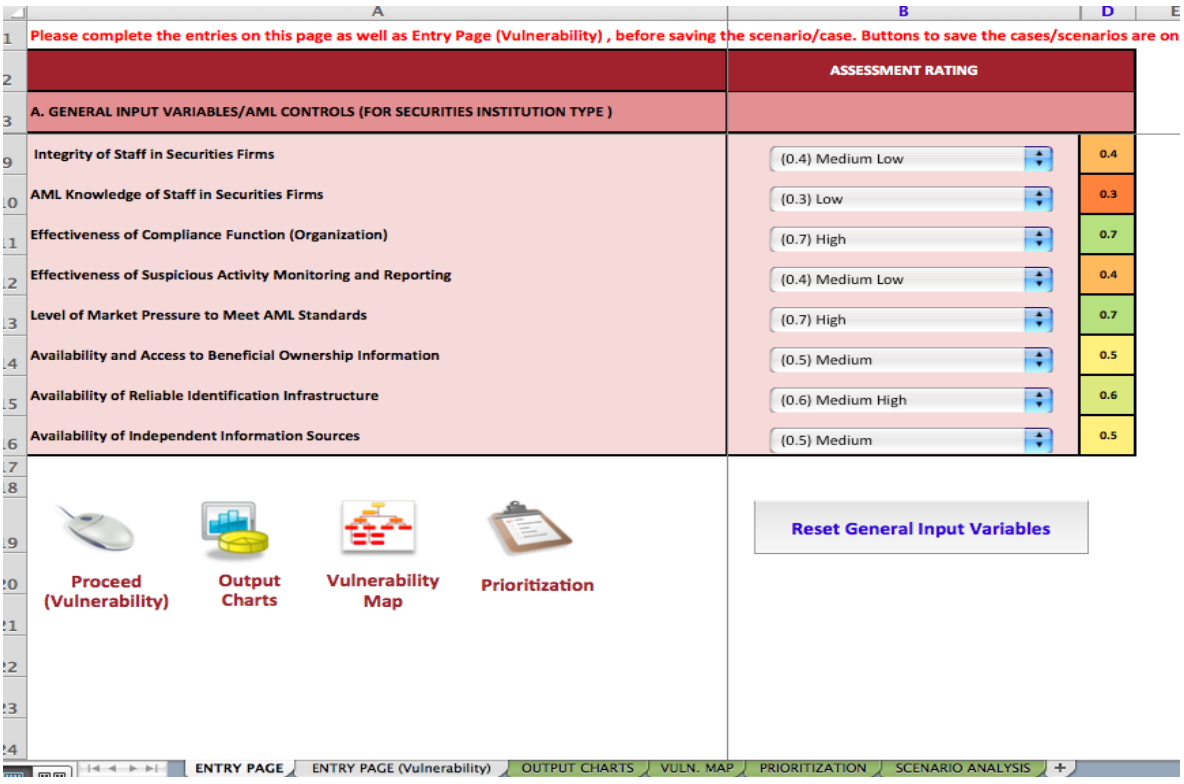
Erase all the entries and restart the process
Click the **Reset Inherent Vulnerability Entries** icon on the Entry Page (Vulnerability) tab (Figure 8), and click the **Reset General Input Variables** icon on the Entry Page tab (Figure 15) to erase all the previous

entries. Also click the **Clean Charts** icon on the Output Charts tab (Figure 10) to erase the previous entries on the Output Charts tab.

Applicable to product-based assessment – (Excel file 4.B)

Click the **Reset Product Entries** icon on the Entry Page (Products) tab (Figure 9), and click the **Reset General Input Variables** icon on the Entry Page tab (Figure 15) to erase all the previous entries. Also click the **Clean Charts** icon on the Output Charts tab (Figure 11) to erase the previous entries on the Output Charts tab.

Figure 15: Icons on the Entry Page tab – (Applicable to both the Excel files – 4.A and 4.B)



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

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

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

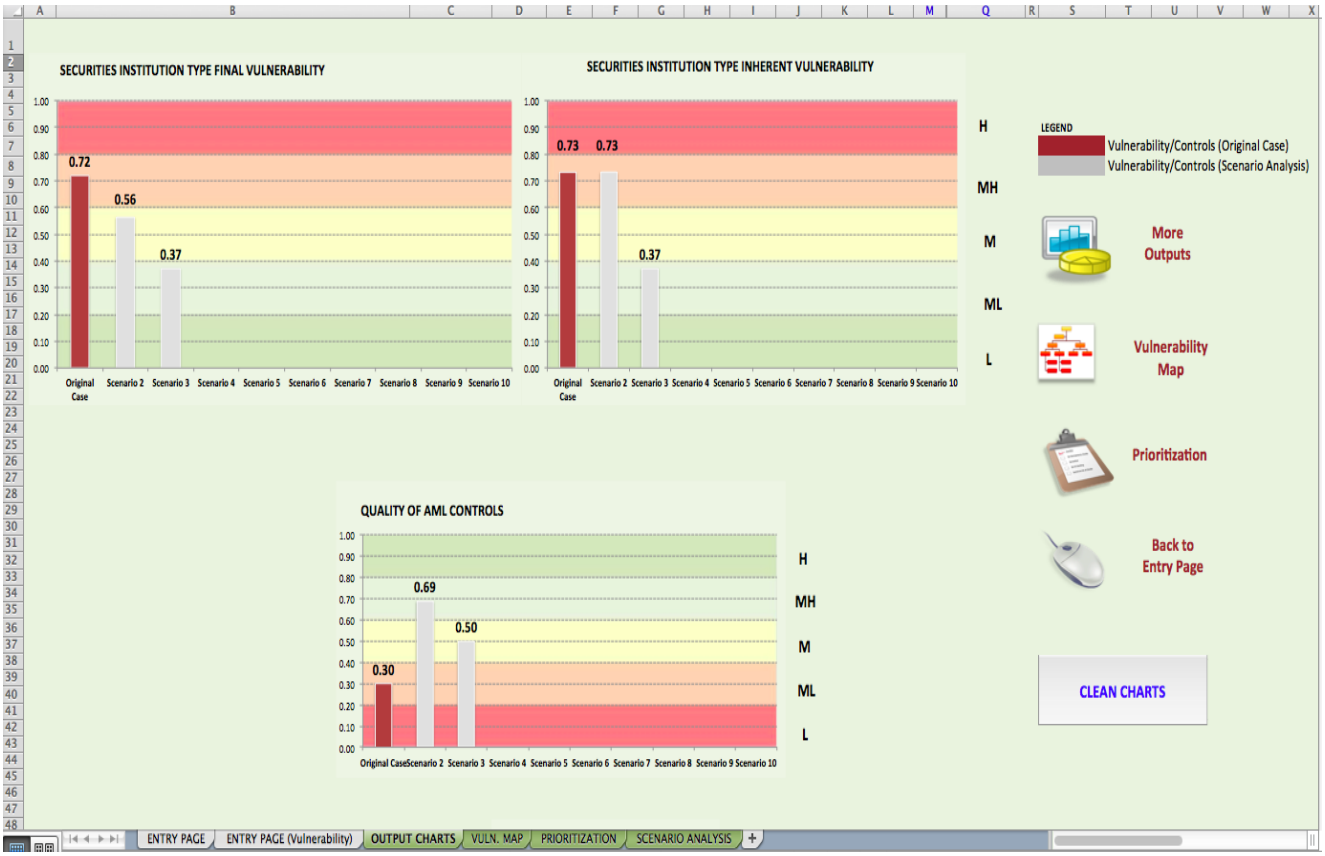
In case of product-based assessment (Excel file 4.B), it can also be used for comparing the final and inherent vulnerabilities of the products for different years or scenarios. It is also possible to use the scenario analysis function for comparing the results of Open Door and Weighted Average Approaches.

Instructions for using the scenario analysis option – Excel file 4.A

To use the scenario analysis option, first be sure to save the Excel file with the original entries, and then create a new copy of the file for scenario analysis. Then go to the Entry Page tab, and make sure you do not reset the entries. Insert the new assessment ratings for the general input variables and inherent vulnerability variables for the second year, or for Scenario 2, in the Entry Page tab and Entry Page (Vulnerability) tab respectively and save the entries as Scenario 2 (as shown in Figure 8).

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

Figure 16: Output Charts – Scenario Analysis (Excel file 4.A)

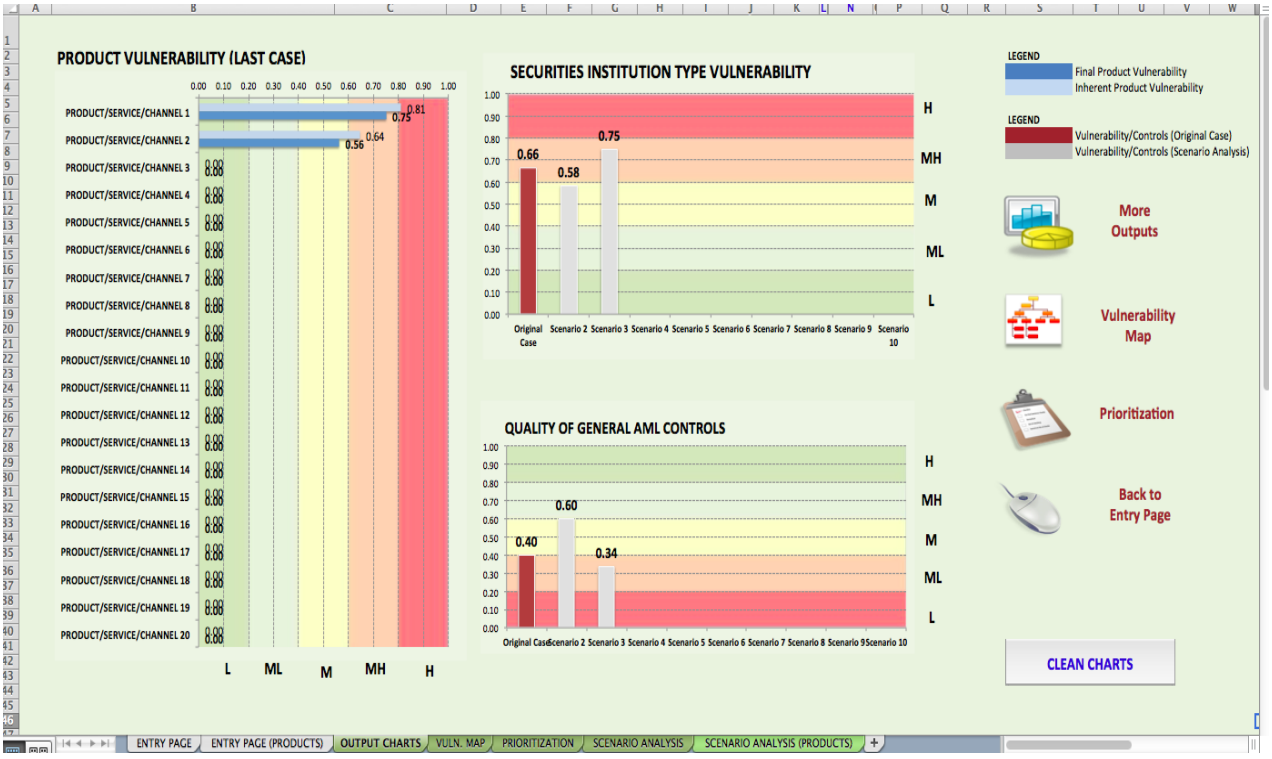


Instructions for using the scenario analysis option for product-based assessment – Excel file 4.B

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

As in Step 5, assessment results are generated in the Output Charts tab (as shown in Figure 17). Note that in a scenario analysis, the original case results are shown in brown while all scenario 2/second year results are shown in gray (see Figure 17). Scenario analysis can be performed for 10 years, or for 10 different scenarios. In Figure 17, the vulnerability assessment results of the products are produced only for the last case (i.e., the third year/Scenario 3). The assessment results for the vulnerability of the assessed securities institution type and the intermediate variables (such as *Quality of AML Controls* and *Quality of Operations in Securities Firms*) are available for all the previous cases, as well as the last case (as shown in Figure 17).

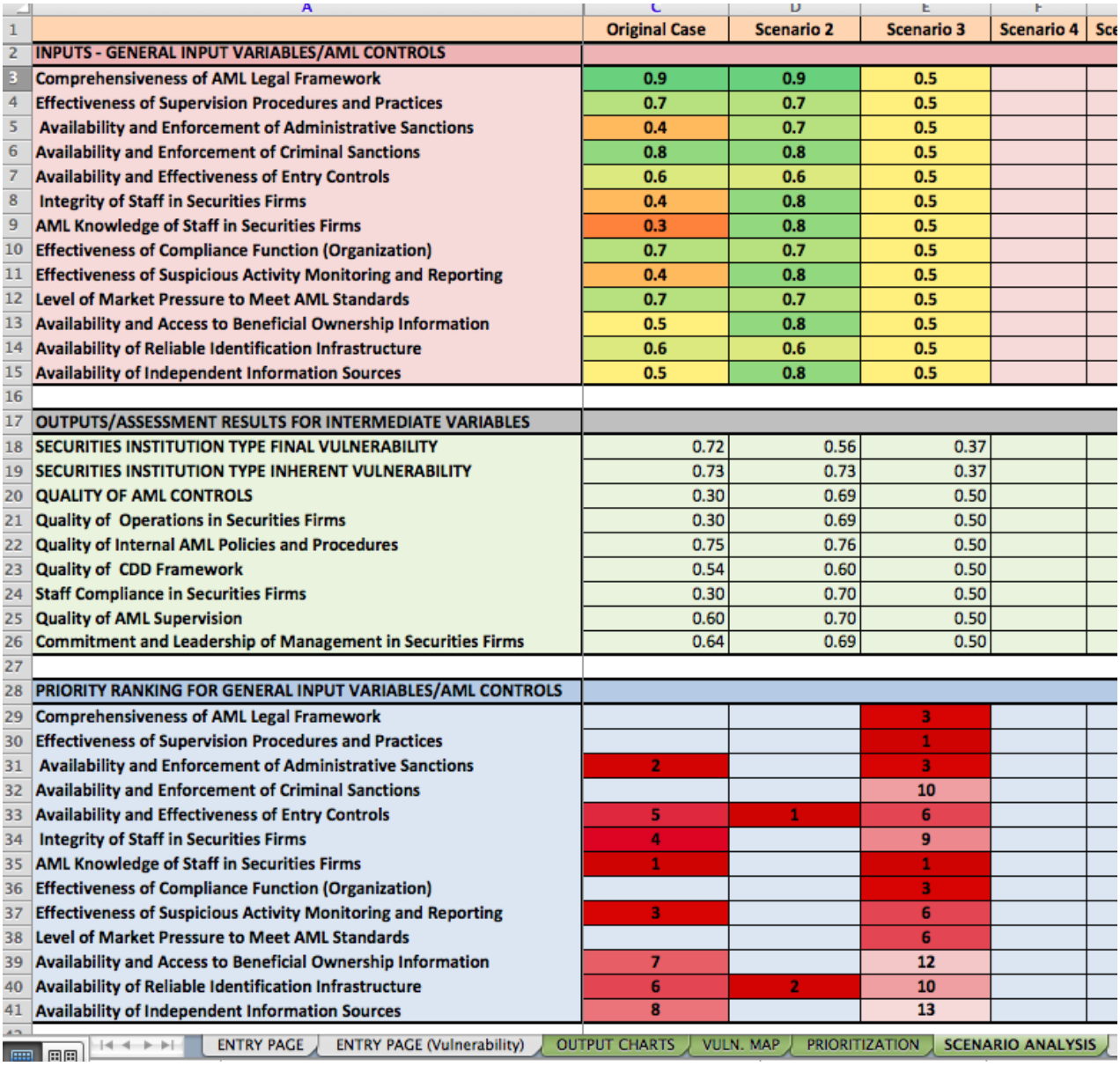
Figure 17: Output charts – Scenario Analysis (Excel file 4.B)



Scenario Analysis results – screen display (Excel file 4.A)

The Scenario Analysis tab provides the assessment results for the different years or scenarios (Figures 18). The Scenario Analysis tab shows the assigned assessment ratings for the general input variables, the assessment results for intermediate variables, the final and inherent vulnerability of the assessed securities institution type, and the priority rankings of the general input variables for the various years/scenarios. These tables are helpful in understanding where changes in the vulnerability of the assessed securities institution type originate, as well as the impact of policy actions on vulnerability, the combating ability/AML controls and the priority ranking of general input variables. The tables show how policy actions have an impact on the various components of vulnerability over a period of time, or in different scenarios.

Figure 18: Scenario Analysis tab (Excel file 4.A)



		Original Case	Scenario 2	Scenario 3	Scenario 4	Sce
2	INPUTS - GENERAL INPUT VARIABLES/AML CONTROLS					
3	Comprehensiveness of AML Legal Framework	0.9	0.9	0.5		
4	Effectiveness of Supervision Procedures and Practices	0.7	0.7	0.5		
5	Availability and Enforcement of Administrative Sanctions	0.4	0.7	0.5		
6	Availability and Enforcement of Criminal Sanctions	0.8	0.8	0.5		
7	Availability and Effectiveness of Entry Controls	0.6	0.6	0.5		
8	Integrity of Staff in Securities Firms	0.4	0.8	0.5		
9	AML Knowledge of Staff in Securities Firms	0.3	0.8	0.5		
10	Effectiveness of Compliance Function (Organization)	0.7	0.7	0.5		
11	Effectiveness of Suspicious Activity Monitoring and Reporting	0.4	0.8	0.5		
12	Level of Market Pressure to Meet AML Standards	0.7	0.7	0.5		
13	Availability and Access to Beneficial Ownership Information	0.5	0.8	0.5		
14	Availability of Reliable Identification Infrastructure	0.6	0.6	0.5		
15	Availability of Independent Information Sources	0.5	0.8	0.5		
16						
17	OUTPUTS/ASSESSMENT RESULTS FOR INTERMEDIATE VARIABLES					
18	SECURITIES INSTITUTION TYPE FINAL VULNERABILITY	0.72	0.56	0.37		
19	SECURITIES INSTITUTION TYPE INHERENT VULNERABILITY	0.73	0.73	0.37		
20	QUALITY OF AML CONTROLS	0.30	0.69	0.50		
21	Quality of Operations in Securities Firms	0.30	0.69	0.50		
22	Quality of Internal AML Policies and Procedures	0.75	0.76	0.50		
23	Quality of CDD Framework	0.54	0.60	0.50		
24	Staff Compliance in Securities Firms	0.30	0.70	0.50		
25	Quality of AML Supervision	0.60	0.70	0.50		
26	Commitment and Leadership of Management in Securities Firms	0.64	0.69	0.50		
27						
28	PRIORITY RANKING FOR GENERAL INPUT VARIABLES/AML CONTROLS					
29	Comprehensiveness of AML Legal Framework			3		
30	Effectiveness of Supervision Procedures and Practices			1		
31	Availability and Enforcement of Administrative Sanctions	2		3		
32	Availability and Enforcement of Criminal Sanctions			10		
33	Availability and Effectiveness of Entry Controls	5	1	6		
34	Integrity of Staff in Securities Firms	4		9		
35	AML Knowledge of Staff in Securities Firms	1		1		
36	Effectiveness of Compliance Function (Organization)			3		
37	Effectiveness of Suspicious Activity Monitoring and Reporting	3		6		
38	Level of Market Pressure to Meet AML Standards			6		
39	Availability and Access to Beneficial Ownership Information	7		12		
40	Availability of Reliable Identification Infrastructure	6	2	10		
41	Availability of Independent Information Sources	8		13		

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

Scenario Analysis results – screen display for product-based assessment – (Excel file 4.B)

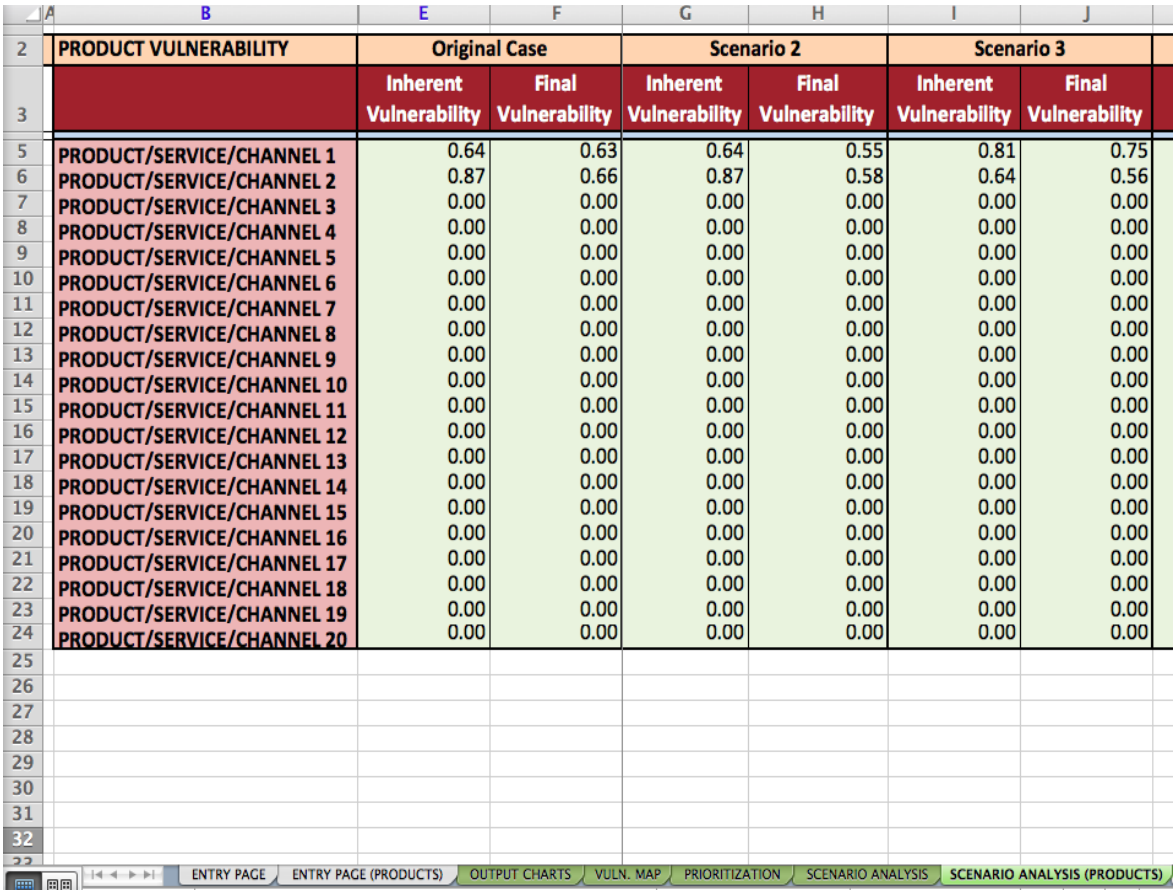
The Scenario Analysis tab and the Scenario Analysis (Products) tab provide the assessment results for the different years or scenarios (Figures 19 and 20). The Scenario Analysis tab shows the assigned assessment ratings for the general input variables, the assessment results for intermediate variables, the vulnerability of the assessed securities institution type, 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 assessed securities institution type originate, as well as the impact of policy actions on vulnerability, the combating ability/AML controls, the product vulnerability, and the priority ranking of general input variables. The tables show how policy actions have an impact on the various components of vulnerability over a period of time, or in different scenarios.

Figure 19: Scenario Analysis tab – (Excel file 4.B)

	Original Case	Scenario 2	Scenario 3	Scenario 4	Sce
INPUTS/GENERAL INPUT VARIABLES					
Comprehensiveness of AML Legal Framework	0.8	0.8	0.2		
Effectiveness of Supervision Procedures and Practices	0.6	0.6	0.5		
Availability and Enforcement of Administrative Sanctions	0.5	0.8	0.6		
Availability and Enforcement of Criminal Sanctions	0.3	0.8	0.6		
Availability and Effectiveness of Entry Controls	0.3	0.8	0.6		
Integrity of Staff in Securities Firms	0.8	0.8	0.5		
AML Knowledge of Staff in Securities Firms	0.4	0.9	0.6		
Effectiveness of Compliance Function (Organization)	0.6	0.6	0.3		
Effectiveness of Suspicious Activity Monitoring and Reporting	0.8	0.8	0.6		
Level of Market Pressure to Meet AML Standards	0.7	0.7	0.4		
Availability and Access to Beneficial Ownership Information	0.7	0.7	0.4		
Availability of Reliable Identification Infrastructure	0.5	0.9	0.2		
Availability of Independent Information Sources	0.3	0.7	0.7		
OUTPUTS/ASSESSMENT RESULTS FOR INTERMEDIATE VARIABLES					
SECURITIES INSTITUTION TYPE VULNERABILITY	0.66	0.58	0.75		
QUALITY OF GENERAL AML CONTROLS	0.40	0.60	0.34		
Quality of Operations in Securities Firms	0.40	0.60	0.49		
Quality of Internal AML Policies and Procedures	0.64	0.70	0.34		
Quality of CDD Framework	0.50	0.79	0.20		
Staff Compliance in Securities Firms	0.40	0.60	0.50		
Quality of AML Supervision	0.57	0.60	0.50		
Commitment and Leadership of Management in Securities Firms	0.51	0.69	0.51		
PRIORITY RANKING FOR GENERAL INPUT VARIABLES					
Comprehensiveness of AML Legal Framework			2		
Effectiveness of Supervision Procedures and Practices	2	1	1		
Availability and Enforcement of Administrative Sanctions	4		8		
Availability and Enforcement of Criminal Sanctions	5		12		
Availability and Effectiveness of Entry Controls	3		9		
Integrity of Staff in Securities Firms			7		
AML Knowledge of Staff in Securities Firms	1		4		
Effectiveness of Compliance Function (Organization)	6	2	3		
Effectiveness of Suspicious Activity Monitoring and Reporting			9		
Level of Market Pressure to Meet AML Standards			5		
Availability and Access to Beneficial Ownership Information			11		
Availability of Reliable Identification Infrastructure	7		6		
Availability of Independent Information Sources	8				

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

Figure 20: Scenario Analysis (Products) tab – (Excel file 4.B)



PRODUCT VULNERABILITY	Original Case		Scenario 2		Scenario 3	
	Inherent Vulnerability	Final Vulnerability	Inherent Vulnerability	Final Vulnerability	Inherent Vulnerability	Final Vulnerability
PRODUCT/SERVICE/CHANNEL 1	0.64	0.63	0.64	0.55	0.81	0.75
PRODUCT/SERVICE/CHANNEL 2	0.87	0.66	0.87	0.58	0.64	0.56
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

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

How to "unhide" the Weights tab

The default weights of the variables and 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.

Figure 21: Weights tab – (Applicable to both the Excel files – 4.A and 4.B)

	A	B	C
1	NOTICE! Data on this page contains the assumptions of the model and can be edited only by Authorized Users		
2	VULNERABILITY OF THE SECURITIES INSTITUTION TYPE	WEIGHTS	PREREQUISITES
3	1. AML CONTROLS FOR THE SECURITIES INSTITUTION TYPE (QUALITY OF AML CONTROLS)	2	0
5	1.1. Quality of Operations in Securities Firms	1	1
6	1.1.1. Quality of CDD Framework	1	0
7	1.1.1.1. Availability of Reliable Identification Infrastructure	3	1
8	1.1.1.2. Availability and Access to Beneficial Ownership information	3	0
9	1.1.1.3. Availability of Independent Information Sources	1	0
10	1.1.2. Effectiveness of Suspicious Activity Monitoring and Reporting	2	0
11	1.1.3. Staff Compliance in Securities Firms	3	1
12	1.1.3.1. Integrity of Staff in Securities Firms	2	0
13	1.1.3.2. AML Knowledge of Staff in Securities Firms	3	1
14	1.1.3.3. Effectiveness of Compliance Function	2	0
15	1. 1.3.4. Quality of AML Supervision	2	1
16	1.1.3.4.1. Effectiveness of Supervision Procedures and Practices	2	1
17	1.1.3.4.2. Availability and Enforcement of Administrative Sanctions	1	0
18	1.1.3.5. Availability and Enforcement of Criminal Sanctions	1	0
19	1.1.4. Commitment and Leadership of Management in Securities Firms	3	1
20	1.1.4.1. Quality of AML Supervision	4	0
21	1.1.4.2. Level of Market Pressure to Meet AML Standards	2	0
22	1.1.4.3. Availability and Effectiveness of Entry Controls	2	0
23	1.1.4.4. Availability and Enforcement of Criminal Sanctions	1	0
24	1.2. Quality of Internal AML Policies and Procedures	1	1
25	1.2.1. Comprehensiveness of AML Legal Framework	1	0
26	1.2.2. Commitment and Leadership of Management in Securities Firms	1	0
27	1.2.3. Effectiveness of Compliance Function	1	0
32	2. INHERENT VULNERABILITY OF THE SECURITIES INSTITUTION TYPE	3	1
33	2.1. Total Value/Size	3	
34	2.2. Complexity and Diversity of the Portfolio	3	
35	2.3. Client Base Profile	3	
36	2.4. Existence of Investment/Deposit Feature	1	
37	2.5. Liquidity of the Portfolio	2	
40	2.6. Frequency of International Transactions	2	
41	2.7. Other Vulnerable Factors	3	
49			

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

In Figure 21, Column B shows the weights for the variables in the Excel file. The weights assigned to the variables are relative. For example, the variable *Quality of Operations in Securities Firms* (line 5) is determined by four variables:

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

The weights on these four variables in determining the *Quality of Operations in Securities Firms* (line 5) are relative to one another, as follows. The weight of the variable *Staff Compliance in Securities Firms* (line 11) is three times that of the variable *Quality of CDD Framework* (line 6), while the variable *Quality of AML Controls* (line 3) is determined equally by the variables *Quality of Operations in Securities Firms* (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 21). 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.

ANNEX 2 – PRODUCT-BASED ASSESSMENT MODULE (Module 4.B)

The Working Group (WG) can decide to undertake a more detailed assessment of the products being offered by the assessed securities institution type. This is to be decided on a needs basis, which is based on the relevance of the institution type, and the number of different products that may be offered by that institution type. Only assess different products within the institution type if the products have different money laundering risks and there are benefits to be derived from detailed separate product analysis.

As discussed in Section 2.2, there are two types of variables in this module: (1) input variables, and (2) intermediate variables.

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

    a. ***AML control variables*** are also broken down into two subtypes: (1) General AML controls, and (2) Product Specific AML controls.

        i. *General AML controls:* These apply to the entire securities institution type, and should be assessed at the institution type level. This type of input variable determines 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 impact only the vulnerability of the product they are related to.

    b. ***Inherent vulnerability variables*** relate to specific features and users of a particular product because they reflect the type/nature of products that make up the assessed institution type. 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 risks related to the client profiles separately for different products.

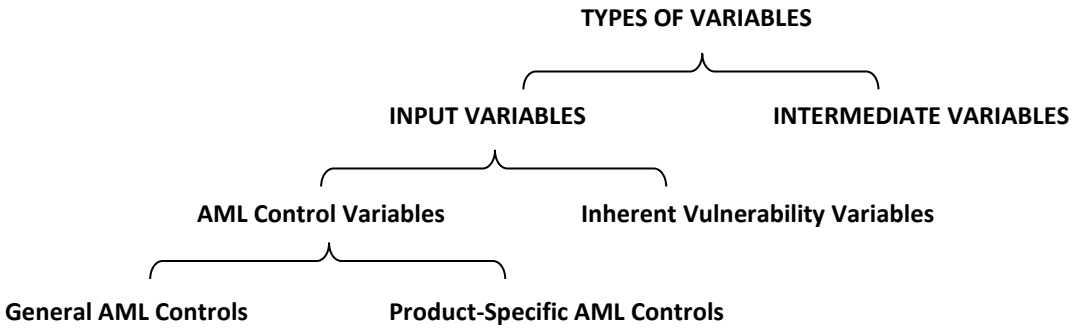
2. **Intermediate variables** are broad and high-level factors that cannot be assessed directly. They therefore need to be disaggregated into their constituent parts in order to be assessed. The module determines intermediate variables automatically, based on the ratings entered for the input variables.

General AML control variables relate to the effectiveness of the general AML controls, and are relevant for all products (of the assessed institution type). This is because an institution type that is well supervised for AML purposes by well-trained and committed officials has reduced vulnerability on all the products being offered.

Other input variables relate to inherent vulnerability factors that are specific to a particular product: e.g., the total value/size 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 Controls*.
Figure 22 provides a visual summary of the variable types.

Figure 22: Variables in the Product-Based Securities Sector Vulnerability Module



The relationship between this breakdown and the module structure in Figure 23 is as follows (see colored boxes in Fig. 23):

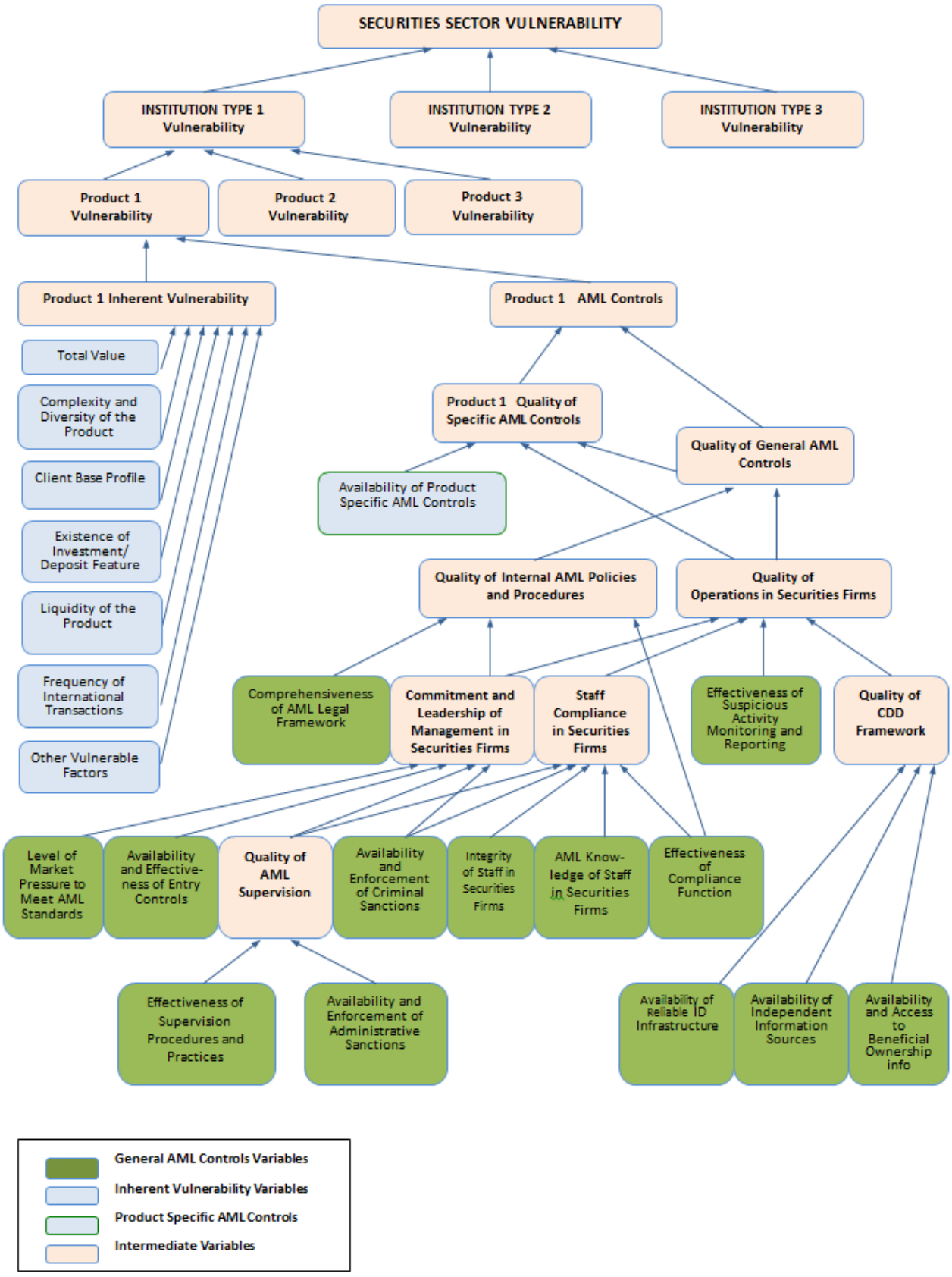
- Intermediate variables (pink boxes) do not require assessment.
- General AML control variables (green boxes) need to be assessed for the entire securities institution type.
- Inherent vulnerability variables (blue boxes) need to be assessed for each product of the assessed securities institution type.
- Product-specific AML controls[2] (blue box with green border) need to be assessed for each product of the assessed securities institution type.

Module Structure (The Network)

As illustrated in Figure 23, the overall vulnerability of the securities sector is determined by the vulnerabilities of the different institution types being assessed. Assessing the vulnerabilities of existing securities institution types therefore contributes to a comprehensive assessment of the vulnerability of the securities sector as a whole. The overall vulnerability of the institution type is determined by the vulnerabilities of the various products assessed for the institution type. 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). "Institution Type 1" and "Product 1" are used as examples in Figure 23. Similar assessments can be performed for other securities institution types, and up to 20 products for each institution type can be assessed.

Figure 23: Product-Based Securities Sector Vulnerability Module structure (Excel file 4.B)

[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.


SECURITIES SECTOR VULNERABILITY
INSTITUTION TYPE 1 Vulnerability
INSTITUTION TYPE 2 Vulnerability
INSTITUTION TYPE 3 Vulnerability
Product 1 Vulnerability
Product 2 Vulnerability
Product 3 Vulnerability
Product 1 Inherent Vulnerability
Product 1 AML Controls
Total Value
Complexity and Diversity of the Product
Client Base Profile
Existence of Investment/ Deposit Feature
Liquidity of the Product
Frequency of International Transactions
Other Vulnerable Factors
Product 1 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 Operations in Securities Firms
Comprehensiveness of AML Legal Framework
Commitment and Leadership of Management in Securities Firms
Staff Compliance in Securities Firms
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 Staff in Securities Firms
AML Know-ledge of Staff in Securities Firms
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
Inherent Vulnerability Variables
Product Specific AML Controls
Intermediate Variables

Guidance for Assessment of Variables

For the assessment of general AML control variables, refer to Section 4.1, where you can find assessment worksheets for AML control variables. The criteria for assessing general AML control variables are the same as the criteria for assessing AML control variables for the specific institution type. Similarly, the criteria for assessing inherent vulnerability variables for each product are the same as the criteria for assessing broader inherent vulnerability factors for the specific institution type. For assessment worksheets on inherent vulnerability variables, refer to Section 4.2.

Inherent factors may differ among the products; we therefore need to assess the inherent vulnerability of each product separately. The vulnerability of a product will also depend on the availability of additional AML controls that are specific to that particular product. These additional AML controls are called Product-specific AML controls, which are explained later in this section.

Suggested list of 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:

- Bearer shares/securities
- Exchange-traded derivatives
- Registered collective investment schemes
- Unregistered collective investment schemes
- OTC derivatives
- Other liquid instruments
- Other illiquid instruments.

The WG may decide to break down some of these products further, if it feels that different sub-categories within a product may pose different ML risks. All significant products and any new, unique, or unusual products – even if their volume is not necessarily significant – should (as far as possible) be included in the assessment.

Assessment Worksheet for *Product-Specific AML Controls*

Certain products are more inherently vulnerable to money laundering than others. 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 from clients – such as PEPs or high-wealth individuals who typically use the product. To assess whether the incidence of such products affects the overall vulnerability of the securities institution type, 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 assessed institution type may have some specific red-flag indicators that focus on large wealth managers; or may require additional customer identification or monitoring procedures for clients of large wealth managers. These additional AML controls reduce the vulnerability arising from large wealth managers, and help reduce the overall vulnerability in the assessed securities institution type.

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 only needed if there are 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 during delivery of a particular product in the securities institution type.

Specific AML controls are controls that are applied, in addition to general AML controls, to all the products offered by a particular type of securities institution. Securities firms that implement specific AML controls may reduce their vulnerability to money laundering.

Assessment criteria

Specific AML controls for a product in a securities institution type are in place if:

- Securities firms generally implement an effective risk-based approach to AML.
- Securities firms 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 (specify references to particular products)
- Data/information on the use of specific AML controls for a product from the assessed institution type
- Findings of AML on-site/off-site examinations
- Interviews/consultations with representatives from the institution type (including professional bodies and voluntary associations)
- Interviews/consultations with supervisory authorities
- Surveys of management and staff from securities firms (of the institution type being assessed)
- Interviews with, and data compiled by, private sector research or consulting firms

Additional guidance

If the product of the assessed institution type is not subject to any specific AML controls, then select the option **Only General AML Controls exist**. For many products, general AML controls may be adequate for risk mitigation. Not having specific controls does not necessarily constitute a problem for a product, particularly for one with low or medium ML vulnerability. The existence of specific AML controls for all products may indicate a high level of ML vulnerability for the institution type. It is unlikely that all the products of an institution type should require specific AML controls. Some products require only general AML controls and do not need specific AML controls because of low/medium ML vulnerability.

One of the objectives of the product risk assessment is to identify whether a product needs specific AML controls or not.

While assessing the need for specific AML controls for a product in the securities institution type, the WG should first assess the ML vulnerability of the product and should understand the main cause of the vulnerability. For example, if a product has high vulnerability to ML due to non-face-to-face use of the product, specific AML controls should be introduced only to reduce non-face-to-face use of the product. These specific AML controls for non-face-to-face use of the product will help to reduce the vulnerability of the product.

Specific AML controls may be required by law/regulations, or firms may apply them voluntarily without an obligation to do so. During the assessment, WG needs to take into account the situation of all the securities firms within the assessed institution type as much as possible. 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.

Note that specific AML controls do not refer to other controls aimed at the elimination of credit risk, fraud risk, or other operational risks. As their objective is different, these types of controls may not always contribute to the elimination of ML risk. The WG can take into account these types of controls, but only in limited conditions – namely when they contribute to reducing ML risk.

For example, in a product of an institution type, specific AML controls may include the following:

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

Summary of the product assessments: Considering the assessment criteria and guidance, assess the availability of specific AML controls associated with each product. For each product, check (✓) the appropriate option in the table. The list of products may be amended as needed.		Product 1	Product 2	Product 3	Product 4	Product 5
Availability of Specific AML Controls	Exist and Comprehensive					
	Exist but Limited					
	Only General AML Controls					