WORLD BANK GROUP
Finance & Markets

NATIONAL RISK ASSESSMENT TOOL
GUIDANCE MANUAL

MODULE 7
VULNERABILITY OF
DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

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

CONTENTS

Important Reminders for the Working Group

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

1. OBJECTIVES OF THE DNFBP SECTOR VULNERABILITY MODULE

The main objectives of this module are to:

- Identify the vulnerability of each of the (relevant) businesses and professions that make up the country's designated non-financial businesses and professions (DNFBP) sector
- Identify businesses/professions of high vulnerability in the DNFBP sector
- Identify, on a needs basis, the products/services[1] offered by the businesses/professions with high ML vulnerability (see Annex 2)
- Prioritize action plans that will strengthen anti-money laundering controls (AML controls) in the DNFBP sector.

[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."

The outcome of the DNFBP vulnerability assessment is necessary for:

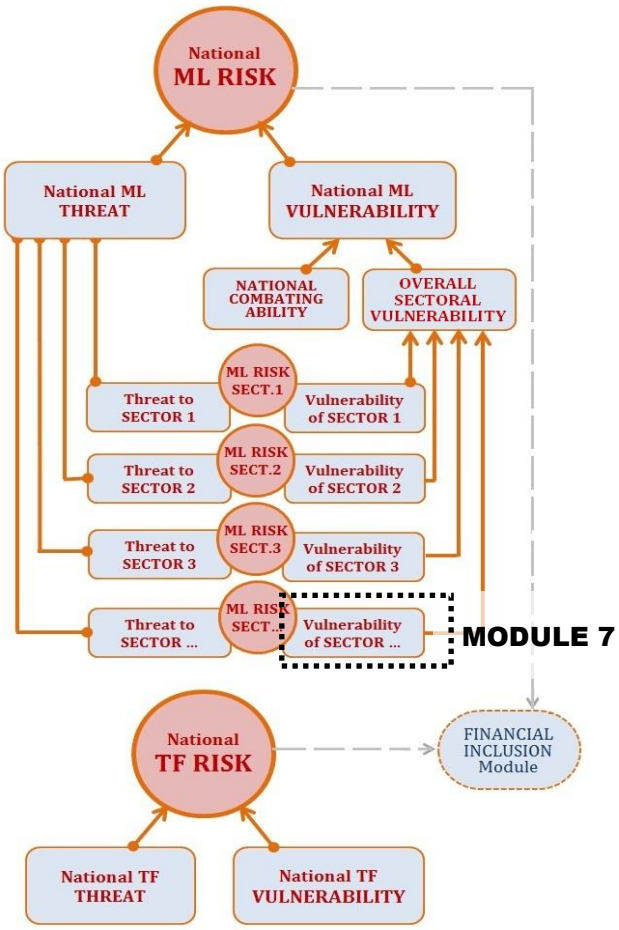
- Designing action plans for more effective AML policies and practices in the sector
- Evaluating the impact of different interventions by regulatory (and other relevant) authorities
- Comparing the level of vulnerability of a business/profession in the DNFBP sector with other businesses/professions, and the vulnerability level of each of the assessed business/profession in relation to other financial sectors
- Ensuring efficient resource allocation
- Developing specific AML controls for high-risk businesses/professions in the DNFBP sector and their products.

2. UNDERSTANDING THE DNFBP VULNERABILITY MODULE

2.1. DNFBP Vulnerability Module in the Big Picture

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

Figure 1: DNFBP Vulnerability Module in the Big Picture of National Risk Assessment Tool



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

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

Please note that the module should be run separately for each of the identified businesses and professions in the DNFBP sector. The final rating of vulnerability for each business/profession will also serve as a separate input to the National Vulnerability module. Figure 1, shows only four sectors as examples. But the number of the sectors that feed into the national vulnerability can be up to 20.

Begin this exercise by making a list of the businesses/professions in the DNFBP sector in your country.

Suggested list of DNFBP businesses/professions

The suggested list of DNFBP businesses/professions has been designed to provide a starting point to the Working Group (WG). The WG is encouraged to modify the list, depending on the country context and the type of businesses/professions present in the country.

Table 1: Proposed list of DNFBP businesses/professions

DNFBP BUSINESSES/ PROFESSIONS	SUGGESTED PRODUCTS TO BE ASSESSED (IF NECESSARY): SEE 2.1 FOR MORE DETAILS
Casinos	• Land-based casinos and gambling houses • On-line (web) gambling.
Real estate agents	Transactions for their clients in buying and selling of real estate
Real estate investors	When conducting transactions for themselves or clients
Dealers in precious metals and stones	Cash transactions with a customer equal to or above the applicable designated threshold
Lawyers, notaries, and other independent legal professionals	When they prepare for or carry out transactions for their client concerning the following activities: • Buying and selling of real estate • Managing of client money, securities, or other assets • Management of bank, savings, or securities accounts • Organization of contributions for the creation, operation or management of companies • Creation, operation, or management of legal persons or arrangements, and buying and selling of business entities.
Accountants, auditors, tax advisers	When they prepare for or carry out transactions for their client concerning the following activities: • Buying and selling of real estate • Managing of client money, securities, or other assets • Management of bank, savings, or securities accounts • Organization of contributions for the creation, operation, or management of companies • Creation, operation, or management of legal persons or arrangements, and buying and selling of business entities.

Trusts and Company Service Providers (TCSPs)	When they prepare for or carry out transactions for a client concerning the following activities: • Acting as a formation agent of legal persons • Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons • Providing a registered office, business address or accommodation, correspondence, or administrative address for a company, a partnership, or any other legal person or arrangement • Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement • Acting as (or arranging for another person to act as) a nominee shareholder for another person.
Other businesses and professions, specific to the country	Products (specify)

Some sub-categories within a product may pose significantly different ML risks. This may be due to factors such as inherent characteristics, client profile or volume, or it may be due to a lack of adequate AML controls for the product. In such cases, the WG may decide to break down these products still further. For example, in the case of the TCSPs and "acting as formation agent of legal persons," the WG will need to consider which forms of legal entity and legal arrangements available in the country are most vulnerable to ML risks (due to their characteristics, and the criteria as laid out in the specific input variables), as well as the AML Controls. Particular attention should be given to products (and services) that allow clients to create "legal distance" between themselves and the assets (e.g., private limited liability companies and express trusts).

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

The WG can decide whether or not to undertake a more detailed assessment of the products provided by each business/profession. This decision should be based on following criteria:

- Does the business/profession provide a single type of product or various products?
- If a business/profession provides various products, does the ML/TF risk differ significantly among the products?
- Is the business/profession significant in the country context?

The more detailed product-based assessment is especially encouraged for legal professionals and TCSPs in financial centers. Up to five different products for each DNFBP business/profession may be assessed.

The assessment of products is carried out in the same way as the assessment of DNFPB business/profession categories. Please note that the assessment criteria detailed in Section 4 also apply in the case of the product-based assessment. For more details on the product-based assessment module, please refer to Annex 2.

Note that two options of the Excel assessment files are provided. The WG must first choose which Excel assessment file is most appropriate for each DNFPB business/profession. The options are:

- Category Vulnerability Assessment
- Detailed Product-Based Assessment.

In case of Category Vulnerability Assessment, use *Excel File 7.A DNFBPs Vulnerability*. If Detailed Product-Based Assessment is undertaken for the business/profession, use *Excel File 7.B DNFPBs Vulnerability Product-Based*.

2.3. Variables

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

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

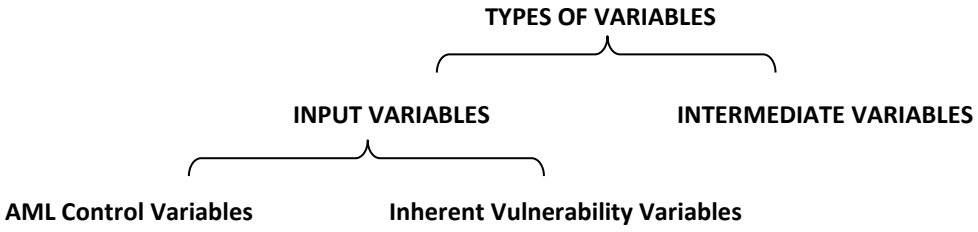
    a. ***AML control variables.*** These factors apply to all assessed businesses/professions in the DNFBP sector, and should be assessed at the business/profession level. These input variables relate to the quality and effectiveness of the AML controls and therefore affect the vulnerability of the entire business/profession being assessed.

    b. ***Inherent vulnerability variables.*** These factors relate to specific features and users of a particular business/profession. An example is the client-base profile. Because the client-base profile for each business/profession may vary (and consequently affect its vulnerability), it is necessary to assess the risks related to the client profile separately for each business/profession.

2. **Intermediate variables** are broad, 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 intermediate variables can be found in Section 5.

Figure 2: Variables in the DNFBP Vulnerability Module

Default: Category Vulnerability (Non-product-based assessment)



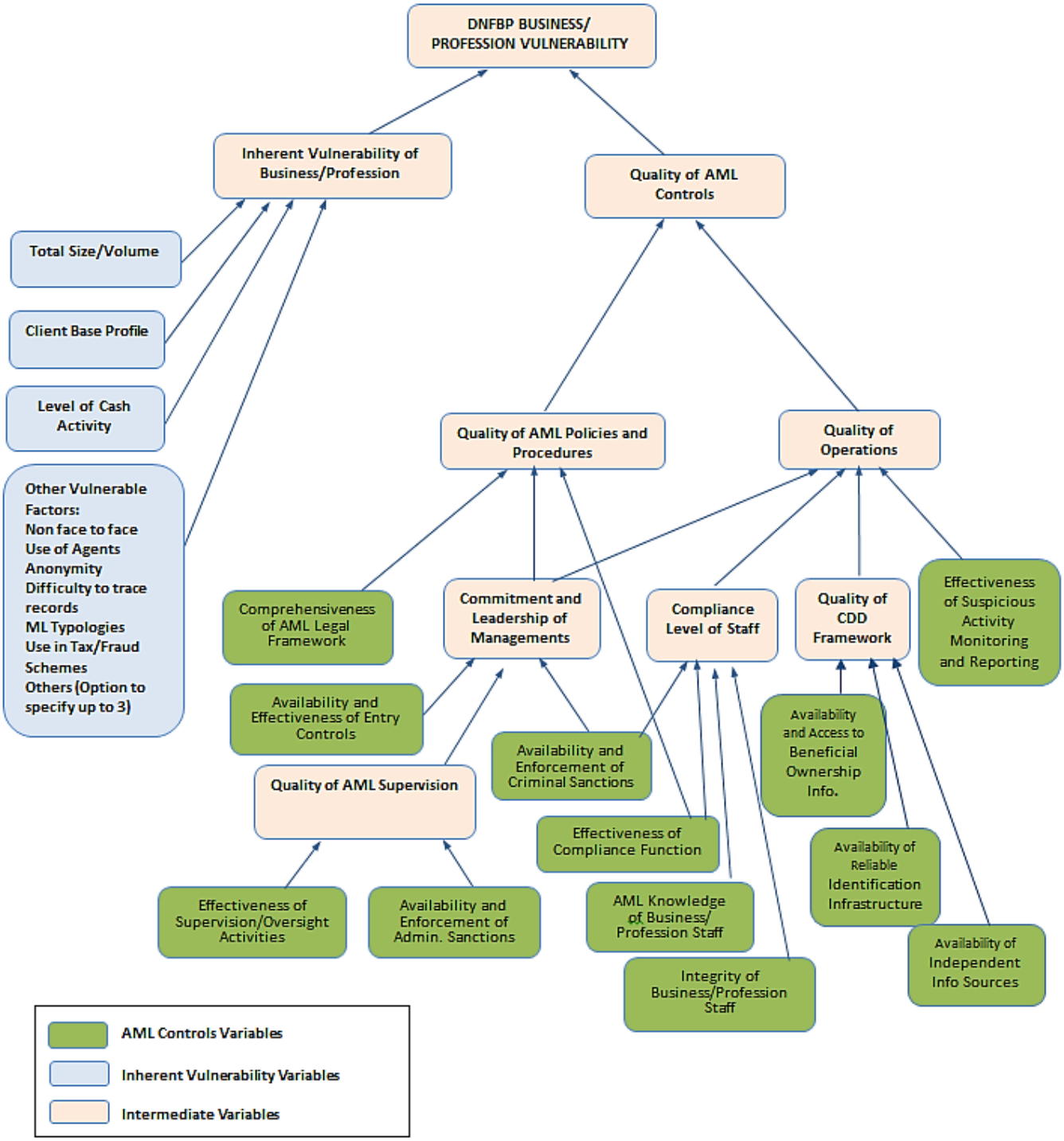
The relationship between this breakdown and the module structure in Figure 3.a is as follows:

- Intermediate variables (pink boxes) do not require assessment.
- AML control variables (green boxes) need to be assessed for the entire DNFBP sector.
- Inherent vulnerability variables (blue boxes) need to be assessed for each business/profession in the DNFBP sector.

2.4. Module Structure (The Network)

As illustrated in Figure 3.a, the vulnerability of the assessed business/profession in the DNFBP sector is determined by a range of inherent vulnerability factors related to the assessed business/profession and a range of AML control factors applied to the assessed business/profession.

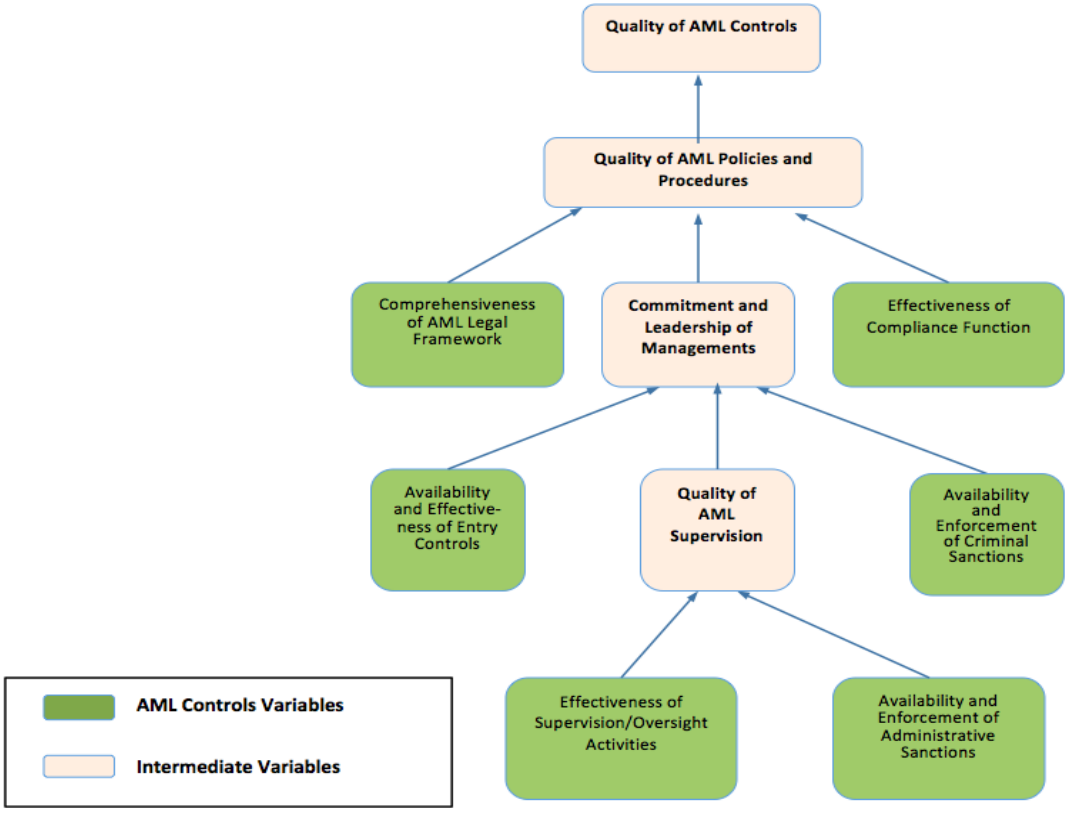
Figure 3.a: DNFBPs Business/Profession (Category) Vulnerability Module (Excel file 7.A)



2.5. The Logic behind the Network

In Figure 3.b, a small part of this 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. 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 *Availability and Enforcement of Administrative Sanctions*. Consider how, in the assessed DNFBP business/profession, the availability and enforcement of administrative sanctions affect the quality of AML controls. Clearly there is an impact, but not a direct impact.

Availability and Enforcement of Administrative Sanctions improves the supervisory authority's ability to apply pressure on an assessed business /profession's managements. This supervisory pressure strengthens the assessed business/profession's managements' commitment to AML compliance and to show leadership in the matter. As a result, the managements take action to improve the quality of their internal AML policies and procedures. As a result, the business/profession starts having better AML controls and its vulnerability decreases.

However, the input variable *Availability and Enforcement of Administrative Sanctions* is not the only factor that determines the quality of supervision. Other factors are also need to be taken into account, such as powers, capacity and the effectiveness of the supervisory agency. These other factors are captured in another input variable, *Effectiveness of Supervision/Oversight Activities*. Assessing these two variables will provide a good assessment of the *Quality of AML Supervision*.

Note that the *Availability and Enforcement of Administrative Sanctions* and *Effectiveness of Supervision/Oversight Activities* are both input variables to the *Quality of AML Supervision*, which is an intermediate variable. Input variables require direct inputs from the WG, while the intermediate variables do not – as illustrated in Figure 3.a (i.e., intermediate variables have arrows feeding into them, while the input variables do not). For descriptions of intermediate variables, see Section 5.

Factors that determine the vulnerability of the business/profession of the DNFBP sector

There are four factors that determine the vulnerability of the business/profession. These are:

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

The assessment ratings of input variables are assigned by the National Risk Assessment Working Groups of the country. The other three items 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 which provide assessment results of intermediate variables based on weighted linking of the underlying relationships of input variables. These formulas can be viewed (i.e., "unhidden") – see Annex 1 for further information. Changes to these formulas can only be made by the World Bank. If changes are required, contact the World Bank NRA Team for further information.

The calculation

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

3. GENERAL GUIDANCE FOR THE ASSESSMENT

3.1. Introduction

The assessments need to be made using the assessment worksheets (see Section 4). Each assessment worksheet describes one input variable and the criteria to consider 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, it 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 influence the business/profession's vulnerability in various directions:

- **AML Controls.** Higher ratings reduce the business/profession's vulnerability; lower ratings increase the business/profession's vulnerability.

- **Inherent Vulnerability Variables.** Higher ratings increase the business/profession's vulnerability; lower ratings decrease the business/profession's vulnerability.

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

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

3.2. Organization of the Assessment Work

The assessment consists of two main stages:

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

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

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

Section 4 and 5 relate to the first stage, while the 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 various modules of the tool, including the DNFBP vulnerability module, and are assessed at a national level. Their assessment ratings should be consistent across all modules, and should be based on systematic and logical reasoning. Although it is sufficient for one WG to assess the ratings of these input variables, it is advised that both the National Vulnerability and Banking Sector Vulnerability WGs assess these variables. It will be useful to compare the assessment ratings assigned by the two groups and to resolve any conflicts that might occur. It is necessary to ensure that assessment ratings are agreed for these three input variables. Unless there is sufficient rationale to assess these separately, the DNFBP Working Group can obtain the ratings for these variables from the National Vulnerability or Banking Sector Working Groups.

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 are to be analyzed, and judgments should be made regarding the current situation.

3.4. Possible Sources of Information and Data

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

- Statistics (national and international)
- Intelligence
- Interviews with relevant authorities/interest groups/market participants
- Focus group meetings with relevant authorities/interest groups/market participants
- Surveys of general public or focus groups
- Reports by international organizations (e.g., United Nations, World Bank Group, International Monetary Fund, World Customs Organization, and World Trade Organization)
- Reports by international standard-setting bodies (e.g., Financial Action Task Force and FATF Style Regional Bodies)
- Reports by governments/think-tanks/civil society organizations/private institutions
- Books/articles/reports based on academic research
- Press/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 for the assessment of each *AML Controls* variable. Each assessment worksheet contains the description of the variable, the assessment criteria, brief guidance on how to support the assessment and a section to record the rating.

The AML control variables of this module relate to the strength of the AML controls. These variables affect the vulnerabilities of all firms and individuals operating within the assessed business/profession. This assessment applies to each DNFBP business and profession as a whole. Please note: This means that all the firms and individuals in the assessed business/profession need to be assessed together per business/profession type. The AML control variables are as follows:

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

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

In order to better understand how these variables impact the vulnerability of the assessed business/profession, please refer to Figure 3.a.

At this stage, the assessment does not focus on vulnerability directly. Rather, the assessment is more about the quality, effectiveness, or level of these variables. Based on these inputs, vulnerability is determined by the module. For example, the assessment should rate how effective the supervisory body is, not how that effectiveness impacts the vulnerability of the assessed business/profession. This basic principle applies to all of the 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 the mutual evaluation report (MER) findings, if relevant. However, this does not mean that the MER findings are binding on the WG. The WG is encouraged to make use of these and other reports and analyses that assess the ML risks of the country.

Recording the grounds of the assessment

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

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

Completing the Entry Page tab in the Excel file

The results of the AML controls assessment should be filled in on the **Entry Page** tab in the assessed business/profession Excel file. This should be done only after the assessments of all the variables are completed. Please refer to the 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 AML laws and regulations regarding AML preventive measures and AML supervision for the assessed business/profession. (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 on preventive measures and supervision in force for the assessed business/profession if they conform to international standards on:

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

Possible sources of information and data

- Relevant laws, regulations, and enforceable guidance related to the above assessment criteria
- Interviews/consultations with regulatory/supervisory authority (may be a Self-Regulatory Body [SRB]) and other competent authorities
- Interviews/consultations with assessed business/profession's representatives, including a SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession.

Assessment

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

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

4.1.2. Effectiveness of Supervision/Oversight Activities

Variable Description

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

(This variable does not assess the availability and enforcement of sanctions. Sanctions are assessed below as two separate variables on administrative and criminal sanctions.)

Assessment Criteria

The AML supervision/oversight activities are effective where the supervisory body (which can be a self-regulatory body or both, depending on country practice):

- Is clearly identified in the laws and regulations and has appropriate authority and mandate to conduct AML compliance supervision
- Carries out its supervisory activities within a comprehensive supervisory framework that includes clear supervision policies, procedures, and manuals
- Possesses good understanding and appreciation for the ML risks of the assessed business/profession
- Has sufficient number of staff and trains the staff and equips them with necessary skills and up-to-date knowledge–including understanding of the nature of the firms and clients and the products of the assessed business/profession–to carry out AML supervision
- Has other necessary resources to ensure AML compliance (such as the technical capacity, budget, and tools)
- Carries out a comprehensive, risk-based supervisory program that consists of on-site and off-site monitoring and on-site inspections on both regularly scheduled cycles and periodic spot-checks (risk-based and as necessary)
- Reports and records the examination results in a systematic way and is able to effectively use these records for policy purposes
- Exercises moral suasion that has a significant impact on the assessed business/profession's management 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 training, knowledge, and skills
- Information on the type(s) and methods of off-site supervision activities and findings
- Statistics on the number of firms/professionals actually being monitored or inspected (on-site/off-site), and information as to scope, frequency, and intensity of the supervision/ oversight activities
- Statistics and information on main findings of on-site/off-site inspections
- Interviews/consultations with regulatory/supervisory authority (may be a Self-Regulatory Body [SRB]) and other competent authorities
- Interviews/consultations with assessed business/profession's representatives, including a SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession.

Assessment

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

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

4.1.3. Availability and Enforcement of Administrative Sanctions

Variable Description

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

This variable also assesses whether the country takes administrative enforcement actions against a firm or individual members of management or staff in case of noncompliance with AML obligations. Consider the number of administrative actions taken against the firms and their staff (of the assessed business/profession) in the last few years for non-compliance of AML obligations.

Assessment Criteria

The following criteria indicate that effective, proportionate, and dissuasive administrative sanctions are in place:

- There is a wide range of administrative sanctions (such as monetary penalties, administrative actions and removal of critical staff, and suspension/revocation of business/professional licenses) in force for noncompliance with AML obligations
- The administrative sanctions are sufficient to positively influence the assessed business/profession's firms' management and staff behavior.

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

- Most persons working in the assessed business/profession believe that administrative enforcement 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 business/profession.

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

Possible Sources of Information and Data

- Specific legal and regulatory provisions on administrative sanctions
- Statistics on numbers (by type) of past administrative enforcement actions by relevant authorities
- Information as to steps taken (or not taken) by the assessed business/profession to remedy infractions
- Interviews/consultations with regulatory/supervisory authority (may be a Self-Regulatory Body [SRB]) and other competent authorities
- Interviews/consultations with assessed business/profession's representatives, including a SRB and professional associations (including as to forms of sanctions they enforce, such as disciplinary hearings or revocation of membership)
- Surveys of management and staff of firms that make up the assessed business/profession.

Assessment

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

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

4.1.4. Availability and Enforcement of Criminal Sanctions

Variable Description

This variable assesses whether the country has a range of effective, proportionate and dissuasive criminal sanctions applicable to natural or legal persons in case 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 to firms (legal persons) and to individual managers and staff in relation to the conduct of their activities within or from the country.

This variable assesses not only the legal framework, but also the actual enforcement actions against firms and individual members of management or staff (of the assessed business/profession) in cases of noncompliance with AML obligations.

Assessment Criteria

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

- There are appropriate criminal sanctions in force for noncompliance with AML obligations.
- Persons in the assessed business/profession regard the criminal sanctions regime as sufficiently dissuasive to positively influence individual behavior patterns.
- Criminal sanctions are also applicable for appropriate ancillary offenses to the offense of money laundering.

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

- Most persons working in the business/profession believe that criminal enforcement action would be initiated in case of noncompliance with AML requirements.
- There is a record of convictions, and criminal enforcement actions taken in the past by law enforcement authorities regarding noncompliance with AML requirements in the assessed business/profession. Consider the number of investigations, prosecutions, and convictions, as well as other available evidence on enforcement.
- The criminal enforcement against the business/profession's firms and their staff with regard to other financial crimes (such as fraud) may also give an idea of the "enforcement perception" of the assessed business/profession.

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 business/profession
- Statistics on criminal enforcement actions carried out by foreign law enforcement and other relevant authorities against the firms and individual members or staff of the assessed business/profession, and whether (and in what form and to what extent) the country provided informal or formal assistance to the investigation and prosecution
- Interviews/consultations with regulatory/supervisory authority (e.g., a Self-Regulatory Body [SRB], law enforcement agency, or prosecuting agency)
- Interviews/consultations with assessed business/profession's representatives, including an SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession.

Assessment

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

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

4.1.5. Availability and Effectiveness of Entry Controls

Variable Description

This variable assesses the availability and effectiveness of entry controls, including licensing, registration or other forms of authorization to operate. A country has effective entry controls if there is a comprehensive legal and regulatory framework, which provides authorities with appropriate powers and sufficient level of staff and other resources to carry out their duties vis-à-vis the assessed business/profession. Effective entry controls help reduce money-laundering vulnerabilities and ensure a higher level of compliance with AML requirements, including preventing systemic problems in the assessed business/profession.

Assessment Criteria

The entry controls are effective if the licensing body:

- Is clearly identified in the laws and regulations
- Possesses good understanding and appreciation for the ML risks of the assessed business/profession
- Effectively carries out its licensing and entry controls duties
- Has a clear and comprehensive framework for licensing and registration requirements for the assessed business/profession, including:
  - A fit and proper test designed to prevent criminals or their associates from being granted a business or professional license or being the beneficial owner of a significant controlling interest in the business or holding a significant management position
  - Appropriate educational and professional certification requirements for key directors and senior management
  - Requirement for all licensees to have adequate AML compliance controls in place, including compliance manuals and appointment of well-qualified internal controls/compliance staff
  - Possesses adequate resources to ensure the quality implementation of entry controls for the assessed business/profession, 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 manual 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 regulatory/supervisory authority (may be a Self-Regulatory Body [SRB]) and other competent authorities
- Interviews/consultations with assessed business/profession's representatives, including a SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession.

Assessment

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

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

4.1.6. Integrity of Business/Profession Staff

Variable Description

This variable assesses whether the directors, managers and staff of the firms (including sole practitioners) 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 that they do not become unwittingly involved as "innocent agents" on behalf of criminals seeking to use their products and specialized knowledge and skills.

If staff members collude with criminals or undermine AML controls by acting corruptly, firms are vulnerable to money laundering abuse. Consider the effectiveness of staff vetting programs in the assessed business/profession; the incidence of disciplinary action for breach of integrity-related rules; and the number of criminal cases against staff members.

Assessment Criteria

Professionals and staff of firms of the assessed business/profession act with integrity if:

- 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 business/profession's staff is low (but consider whether there is underreporting of incidences of integrity failure).
- There is an appropriate mechanism in place to protect the business/profession's managers and staff against any negative consequences as a result of reporting suspicious transactions or other actions to 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 as to staff vetting and training programs (of the assessed business/profession)
- Statistics on integrity breaches by the managers and staff in firms (of the assessed business/profession) and information on disciplinary actions taken
- Statistics on the number of criminal cases, including money laundering cases, concerning staff of the firms in the assessed business/profession
- Findings of firms' (of the assessed business/profession) AML on-site inspections and off-site monitoring
- Statistics on number (and types) of administrative enforcement actions against firms and individuals working in the assessed business/profession
- Review of reports/records of internal control/compliance units in firms of the assessed business/profession
- Historical data of incidents /breaches by staff (kept by firms for operational risk management purposes)
- General levels of integrity or the operating environment in the country (refer, for instance, to the Transparency International Corruption Perceptions Index)
- Assessed business/profession's reputation on involvement in financial crimes, including tax evasion
- Interviews/consultations with a regulatory/supervisory authority, which may be a Self-Regulatory Body (SRB) or other competent authority
- Interviews/consultations with assessed business/profession's representatives, including an SRB (particularly internal control or compliance units) and professional bodies
- Surveys of management and staff of firms that make up the assessed business/profession.

Assessment

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

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

4.1.7. AML Knowledge of Business/Profession Staff

Variable Description

This variable assesses how well the professionals and staff of firms in the assessed business/profession know and understand their duties and responsibilities.

Assessment Criteria

Professionals and staff of firms in the assessed business/profession have the required AML knowledge if:

- There are appropriate AML training programs and materials for professionals/staff.
- Training programs are designed to ensure that all appropriate staff members are trained.
- All professionals and 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 firm conducts business with clients and professional intermediary firms in other jurisdictions, their knowledge should also extend to AML laws and regulations of those jurisdictions. Professionals/staff 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 business/profession and specialized knowledge and skills of its professionals and its products and services.
- Professionals/staff are aware of AML compliance and reporting procedures and obligations.

Possible Sources of Information and Data

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

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 firms (including sole practitioners) in the assessed business/profession have an effective compliance function that is comprehensive, risk-based, and well resourced, with an independent AML compliance function.

Assessment Criteria

The assessed business/profession possesses effective internal AML compliance functions if most firms (including sole practitioners):

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

Possible Sources of Information and Data

- Relevant regulatory framework in relation to the compliance function
- Information on internal compliance function and policies of firms in the assessed business/profession
- Findings of the AML on-site inspections and off-site monitoring
- External (if any) and internal audit reports on adequacy and effectiveness of compliance function
- Statistics on disciplinary actions taken by the firms (of the assessed business/profession) against their staff for breaches of compliance policy
- Statistics on new clients or business declined or business relationship terminated, based on recommendations of the compliance staff
- Interviews/consultations with regulatory/supervisory authority (e.g., an SRB or other competent authority)
- Interviews/consultations with assessed business/profession's representatives, including an SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession.

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 the firms of the assessed business/profession 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 firm with a single branch or for a sole practitioner, while large businesses and firms will require more sophisticated systems. A good record-keeping system is a pre-requisite for an effective monitoring system. Any problems and deficiencies in record keeping should therefore be assessed under this variable.

Assessment Criteria

The firms of the assessed business/profession have adequate and appropriate AML-monitoring and STR reporting systems if:

- The firms have information systems that enable and facilitate the monitoring of client transactions and comparing them against the client's profile.
- Transactional records are available in a format that facilitates AML screening and monitoring.
- The systems support the firms in the assessed business/profession in performing effective PEP screening.
- The systems assist the business/profession and its staff to effectively identify and record all complex, unusual large transactions.
- The systems assist the business/profession and its 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 or rules on professional secrecy and professional/client privilege.

Possible Sources of Information and Data

- Relevant legal and regulatory framework in relation to AML monitoring, record-keeping, and STR reporting obligations of the assessed business/profession
- Findings of AML monitoring and supervision with regard to the effectiveness of the firms' (of the assessed business/profession) STR systems (for example, how many firms are compliant, how many are not compliant, and how this affects the overall effectiveness of the STR system for the assessed business/profession)
- Statistics on the number and quality of STRs filed by the firms/professionals (of the assessed business/profession), including numbers filed "defensively" (after being alerted to suspicious activity or investigation by authorities)
- Statistics on numbers of STRs relating to monitoring lapses, etc., originating from the firms/ professionals (of the assessed business/profession)
- Statistics on numbers of STRs by the firms/professionals (of the assessed business/profession) referred to law enforcement agencies
- Statistics on number of detected complex, unusually large transactions that were recorded by the reporting entity and not reported
- Information on quality and accessibility of the firms' (of the assessed business/profession) transaction and CDD records
- Findings of firms/professionals' AML on-site/off-site supervision
- Interviews/consultations with regulatory/supervisory authority (e.g., an SRB or other competent authority)
- Interviews/consultations with assessed business/profession's representatives, including an SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession.

Assessment

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

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

4.1.10. Availability and Access to Beneficial Ownership Information

Variable description

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

Assessment criteria

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

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

Possible sources of information and data

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

Assessment

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

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

4.1.11. Availability of Reliable Identification Infrastructure

Variable description

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

Assessment criteria

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

The infrastructure may consist of:

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

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

Possible sources of information and data

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

Assessment

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

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

4.1.12. Availability of Independent Information Sources

Variable description

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

Assessment criteria

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

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

Possible sources of information and data

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

Assessment

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

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

4.2. Assessment Worksheets for the Inherent Vulnerability Variables

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

Note: WGs can also decide to assess each business/profession on product-specific input variables. The criteria for assessing these product-specific input variables are the same as the criteria for assessing the broader inherent vulnerability factors for the specific business/profession as a whole. See Annex 2 for more detailed product-based assessment.

This section includes guidance on four inherent vulnerability variables.

Inherent Vulnerability Factors

The following input variables reflect the inherent vulnerability factors:

1. *Total size/volume of the business/profession*
2. *Client-base profile of the business/profession*
3. *Level of cash activity associated with the business/profession*
4. *Other vulnerable factors, including*
    a. *Non-face-to-face engagement of services and ongoing relationship*
    b. *Use of agents*
    c. *Anonymous use of the product*
    d. *Difficult to trace transactions (e.g., use of pooled client trust accounts; professional secrecy laws or ethics rules; attorney/client privilege; legal/professional privilege and work [document]/product privilege)*
    e. *ML typologies on the abuse of the business/profession*
    f. *Use of the business/profession in fraud or tax evasion schemes*
    g. *Other relevant features (specify up to three).*

An important relevant feature that should also be considered is whether the business/profession is not licensed or is unregulated for AML, or whether a particular product can be obtained from (1) an unlicensed, unregulated business/profession, or (2) need not involve any regulated business/profession. For example, some countries require that, in order to form and register a certain type of company, one must use the services of a regulated entity/service provider in that country. In other countries, some types of companies or partnerships may be registered without the involvement of any professional intermediary. These four inherent vulnerability input variables determine the vulnerability for each assessed business/profession. The assessment of these four inputs should be performed for each business/profession separately. Therefore, if the country is assessing 10 businesses/professions, there are (4*10=) 40 inherent variables that will need to be assessed.

Complete the "Entry Page (Vulnerability)" Tab in the Excel file

The results of the assessments of the inherent vulnerability variables need to be entered into the "**Entry Page (Vulnerability)**" tab of the DNFBP Vulnerability Excel file 7.A/7.B. This should be done only after the assessments of all the variables have been completed. Please refer to Annex 1 for detailed instructions on how to use the Excel file.

4.2.1. Total size/volume of the business/profession

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

- 1.A Total Number of Providers
- 1.B Total Number of the Product Provided
- 1.C Total Turnover/Value of the Business/Profession.

1.A Total Number of Providers

Variable Description
This variable assesses the total number of providers (firms and individuals) in the business/profession. This information is taken to be indicative of the level of ML vulnerability that they can introduce into the business/profession (if the relevant risks are not mitigated). For some categories (especially unregulated ones), the actual number of providers may be difficult to determine. In that case, what is required is a judgment as to whether or not the providers are significant to the country's economy.
Assessment Criteria
The objective of this indicator is to assess the importance of a business/profession in the country's economy (compared to the other sectors that are being assessed). The most appropriate indicator of the total number of providers within the business/profession depends on the nature of the product being provided. In other words, if the country licenses company service providers, but unlicensed company services firms or individuals are also permitted to provide such services, efforts should be made to ascertain (even if only a best estimate) the number of both licensed and unlicensed providers. For lawyers and other professionals, consider only the number of those that provide financial intermediary services. It may indicate a problem itself, if the country is not able to identify the number of providers.
Possible Sources of Information and Data
• Data on total number of providers (firms and individuals, licensed and unlicensed) within the assessed business/profession • Interviews/consultations with regulatory/supervisory authority (e.g., an SRB or other competent authority) • Interviews/consultations with assessed business/profession's representatives, including an SRB and professional associations • Surveys of management and staff of firms that make up the assessed business/profession • Interviews with and data compiled by private sector research or consulting firms.
Additional Guidance
Consider also whether the particular product can be provided in the jurisdiction only by licensed businesses or professionals, or (1) Are permitted to be provided by "informal" or unlicensed firms and individuals (including informal trustees such as friends and family who serve as trustees of wills/estates or a business providing company secretarial services without a need for licensing as such); and/or (2) Are not permitted within the jurisdiction, but the product is being provided by "informal" or unlicensed firms and individuals (because of lack of clarity in the laws or regulations or lack of effective enforcement against unlicensed firms or individuals). While assessing the total number of providers, please try to decide whether it is significant or not. If it is significant, rate it as high, if not significant, rate it as low. If you think that it is moderately significant, rate it as medium.

1.B Total Number of the Product provided (if applicable)

Variable Description

This variable assesses the total number of a particular product provided by the assessed business/profession (if applicable). The total number of a particular product may be indicative of the level of ML vulnerability that this product can introduce into the assessed business/profession (if the relevant risks are not mitigated).

The actual number of product provided may be very difficult to determine. What is required is a judgment as to whether or not the scale of the number of the product provided is significant in the assessed country's economy.

Assessment Criteria

The objective of this indicator is to assess the importance of a particular product within the assessed business/profession, in comparison to other products offered by the assessed business/profession.

The most appropriate indicator of the total number of a product in the business/profession depends on the nature of the product being assessed. For some products, the number of transactions, number of clients, number of products created or administered associated with the product can be used as an indicator of the total number of product provided. For example, for real estate agents, the number of properties bought and sold on behalf of clients; for trust service providers, the number of express trusts (product) formed and/or administered (service); for company service providers, the number of legal persons formed (by type of legal person), managed or served as professional nominee shareholders or directors.

Possible Sources of Information and Data

- Data on total number of product provided (official and informal estimates) drawn from official agencies and registries (company, land, property, etc.)
- National statistical office
- Interviews with or data from private sector firms that track the business/profession
- Interviews/consultations with a regulatory/supervisory authority (e.g., an SRB or other competent authority)
- Interviews/consultations with assessed business/profession's representatives, including an SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession
- Interviews with and data compiled by private sector research or consulting firms.

Additional Guidance

While assessing the total number of a product, please try to 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).

1.C Total Turnover/Value of the Business/Profession

Variable Description

This variable assesses the total turnover or the total value or amount of transactions handled by a particular business/profession, which is indicative of the level of ML vulnerability that this business/profession can introduce into DNFBP sector if the relevant risks are not mitigated.

In the cases where the total turnover of the assessed business/profession will be difficult to determine, the assessment may require a judgment as to whether or not the total turnover of the business/profession is significant to the country's economy.

Assessment Criteria

The objective of this indicator is to assess the importance of a particular business/profession in country's economy (compared to the other sectors that are being assessed).

For some categories of businesses/professions, the turnover or in other words the total value of the transactions they are handling may be a more meaningful indicator than the others. In addition to the financial statements, tax records of the country, and business/profession's contribution of the sector to GDP may also give good idea of this indicator. Although, asset size is less meaningful for DNFBPs compared to financial institutions, it may also give an impression of the total value they are handling.

The most appropriate indicator of the total turnover or the value of a business/profession may depend on the nature of the business/profession being assessed.

For business/profession (such as legal professionals and accountants in their management of client money, securities or other assets or acting as trustees of express trusts), it may be more appropriate to use "total assets managed" as an indicator of the total value for such services.

Possible Sources of Information and Data

- Data on total value associated with the business/profession
- Data on total turnover associated with the business/profession
- Data on total assets managed associated with the business/profession
- Data on total amount of fund flows associated with the assessed business/profession
- Interviews/consultations with regulatory/supervisory authority (e.g., an SRB) and other competent authorities
- Interviews/consultations with assessed business/profession's representatives, including an SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession
- Interviews with and data compiled by private sector research or consulting firms.

Additional Guidance

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

4.2.2. Client-base profile of the business/profession

Variable Description

This variable assesses whether the type of client that generally uses the business/profession being assessed increases the risks of money laundering abuse of the assessed business/profession.

Note: The tern "client" here may refer to natural persons or legal persons or arrangements; they may also be end-users of the business/profession or professional intermediary firms through which products are provided to the end-users. All forms of clients should be considered in the assessment.

Assessment Criteria

The client-base profile of the business/profession should be assessed to carry a higher risk if it involves:

- Domestic/international PEPs
- High net-worth individuals
- Nonresident clients, particularly from high-risk jurisdictions
- Clients with foreign business or personal interests
- Clients with business links to known high-risk jurisdictions
- Clients with criminal records or past administrative and/or supervisory actions against them
- Clients that are legal entities or arrangements with a complex, opaque ownership and control structure (including layered ownership and control, multijurisdictional or involve high-risk jurisdictions)
- Clients obtained through introduced business, particularly from unregulated professional intermediaries or regulated PIs in jurisdictions with low AML controls (including CDD and recordkeeping, availability and timely access to beneficial ownership of legal entities and legal arrangements, licensing and supervision, and enforcement)
- Professional intermediaries in jurisdictions with low or no CDD requirements
- Professional intermediaries in high-risk businesses/professions in country context.

Possible Sources of Information and Data

- Regulatory framework for risk-based classification of clients
- Regulatory framework for identifying and monitoring foreign and domestic PEPs
- Any product-related statistics on PEPs and other higher-risk clients
- Data on jurisdictions of origin of end-user clients and professional intermediary firms
- DNFBP sector data by business/profession on transactions with high-risk jurisdictions
- Data on clients obtained through introduced business
- Interviews/consultations with regulatory/supervisory authority (e.g., an SRB or other competent authority)
- Interviews/consultations with assessed business/profession's representatives, including an SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession
- Interviews with and data compiled by private sector research or consulting firms
- Criminal data, including typologies on high-risk clients and ML cases where a business/profession was used for ML by high-risk clients
- Statistics on and information from STRs originating from the business/profession with regard to high-risk clients
- Statistics on the foreign jurisdictions where MLA or informal information sharing requests were received and sent by relevant authorities, including by supervisors, law enforcement, the FIU, and tax authorities.

Additional Guidance

While assessing the client-base profile for each business/profession, please assess whether this business/profession is being used by clients who pose a higher ML risk, when compared to "standard" clients. These high-risk clients will include, politically exposed persons (PEPs), non-residents, high net-worth individuals, opaque or complex legal structures, and so on.

It would be useful to look at the geographical breakdown of the clients and the transactions, including those categorized as "high-risk jurisdictions." Clients and transactions associated with high-risk jurisdictions are likely to be

more vulnerable to money laundering as they are not subjected to adequate AML requirements and it is easier for criminals to move illicit funds to and from these centers into the global financial system.

To assess this variable, the country should determine if the assessed business/profession has put in place appropriate mechanisms to identify and monitor high-risk individuals (including PEPs). If such monitoring/analysis mechanisms are not in place, the business/profession may not be able to provide such information.

Under international standards and national legal frameworks of most countries, DNFBPs, when carrying out certain activities (including acting as financial intermediaries and incorporation services), are required to undertake customer due diligence, which includes verification of the beneficial ownership of legal persons and legal arrangements. Thus, DNFBPs should be able to identify nonresident clients, and determine which kinds of products they use. A more advanced analysis, based on the countries that such non-resident clients originate from, will provide further insight into the risk level.

In some cases, the nature of the product will determine the client-base profile. For example the client-base profile of trusts would be high net-worth individuals. While assessing this indicator, please question how likely it is that this type of business/profession will be abused by criminals, compared to other businesses/professions in the sector. If the likelihood is high, the assessment rating for the client-base profile for this business/profession should be relatively side.

Assessment of this indicator will require judgment, unless the country has appropriate mechanisms for identifying and monitoring high-risk clients (including PEPs). If there is no data that can support the assessment, the Working Group should work on the basis of the worst-case scenario and be conservative in its assessment.

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

4.2.3. Level of cash activity associated with the business/profession

Variable Description
This variable assesses the level of cash activity associated with a specific business/profession, both whether the use of cash is permitted and to what extent that occurs.
Assessment Criteria
Assess whether the use of cash is permitted for the business/profession and the level of cash associated with it. The more the business/profession being assessed is cash-based, the greater its vulnerability to money laundering.
Possible Sources of Information and Data
• Interviews/consultations with regulatory/supervisory authority (e.g., an SRB or other competent authority) • Interviews/consultations with assessed business/profession's representatives, including an SRB and professional associations • Surveys of management and staff of firms that make up the assessed business/profession • Interviews with and data compiled by private-sector research or consulting firms • Criminal data, including ML cases where a business/profession was used for ML because of the possibility of transacting in cash (including payment of fees for service provided).

4.2.4. Other vulnerable factors of the business/profession

Variable Description

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

Assessment Criteria

The presence of the following typical factors may increase the ML vulnerability of the assessed business/profession:

- Use of agents
- Possible anonymous use of the product in the business/profession
- Difficulty in tracing the transactions (including attorney/client privilege and professional secrecy for lawyers and accountants; work [document]/product privilege)
- Existence of ML typologies on the abuse of the business/profession
- Use of the business/profession in tax/fraud schemes
- Non-face-to-face interaction with the client.

For all of the above factors, consider whether there is also an **international dimension** and how that may increase the vulnerability of the business/profession to ML risks. Examples: ML typologies that involve transnational financial crime schemes; and introduced business from professional intermediaries located in foreign jurisdictions.

Possible Sources of Information and Data

- Criminal data, including ML cases where a business/profession was used for ML, indicating vulnerability due to the above-mentioned factors
- Data or statistics and qualitative information from MLA and formal or informal requests from supervisory authorities, law enforcement, the FIU, and tax and other relevant authorities to share information/intelligence
- Interviews/consultations with regulatory/supervisory authority (e.g., an SRB) and other competent authorities
- Interviews/consultations with assessed business/profession's representatives, including an SRB and professional associations
- Surveys of management and staff of firms that make up the assessed business/profession
- Interviews with and data compiled by private-sector research or consulting firms.

Additional Guidance

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

Use of Agents: A further example of a vulnerability factor is the use of agents or other professional intermediaries to deliver the product. In this case, ML vulnerability may be increased due to the weak AML systems of the agents or professional intermediaries (including weak systems of the countries in which they operate or reside). To limit vulnerability, the agents or professional intermediaries should be subjected to adequate AML controls and monitoring/supervision by the principal business/profession in the country providing the product.

Possible anonymous use of the product in the business/profession: Assess whether anonymous use of the product is possible for the assessed business/profession. Also, please consider whether the beneficial owner of the transaction is always identified and verified. Does the business/profession allow for anonymous use (where a firm or an individual known to the assessed business/profession uses the product on behalf of several firms or individuals who are unknown to the business/profession)? Anonymous transactions are vulnerable to money laundering, as the beneficial owner(s) of the funds involved in the transaction is/are not known or are unverified. The transaction is executed for the client on behalf of others. The real owners are not known and hence not subjected to customer due diligence.

Difficulty in tracing the transaction records of the business/profession: Please assess whether transactions executed in the course of delivery of a product by the business/profession are properly recorded and whether access to those records can be readily obtained for CDD/EDD. The difficulty in tracing the records would depend on the quality of the assessed business/profession's AML CDD and record-keeping systems. Consider also, for example, the overbroad application or misuse of professional secrecy and privilege provisions, which may also hinder timely access to relevant records by competent authorities.

Existence of ML typologies on the abuse of the business/profession: Assess whether the business/profession is known for abuse for ML purposes. This does not necessarily need to be in the country context. Please look at the typologies at the global level, regardless of whether it was detected or not detected in the country.

Use of the business/profession in fraud or tax evasion schemes: Assess the use of the business/profession in fraud or tax evasion schemes or other predicate offenses. For this purpose, it may be useful to refer to crime and tax enforcement data to

find the businesses/professions that are most vulnerable to actual and potential misuse. The use of the business/profession in tax evasion or fraud schemes or other predicate offenses may indicate a vulnerability to ML abuse as well.

Non-face-to-face use of the product of the business/profession: Availability of non-face-to-face initiation of a business relationship with respect to a business/profession (or product) raises ML vulnerability. If, for example, an individual is able to secure the product via the internet or telephone with no face-to-face contact with the professional or business, there is ML vulnerability. Even in the cases where non-face-to-face initiation of a product is not allowed, but non-face-to-face use of the product is, there is a possibility of ML vulnerability. But in the second case, the vulnerability of the product can be less, depending on the quality of CDD done during the face-to-face product initiation and existence of other controls that limit the use of the product by persons other than the account holder.

Any other vulnerability factors: Please provide any other factor(s) that may render a particular business/profession vulnerable to money laundering. For example, are there complexity features to a product that present challenges in conducting CDD, including verifying beneficial ownership?

Summary of the assessment of the Business/Profession:

Considering the assessment criteria and guidance, assess the inherent vulnerability variables associated with the assessed business/profession. For each business/profession, check (✓) the appropriate option in the table. Repeat this for each business/profession assessed.

			Business/Profession (Module 7.A) Product 1 (Module 7.B)	Product 2 (Module 7.B)	Product 3 (Module 7.B)	Product 4 (Module 7.B)	Product 5 (Module 7.B)
1. A, B, C ***Total size/volume***		High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Not Analyzed					
2. *Client base profile*		Very High Risk					
		High Risk					
		Medium Risk					
		Low Risk					
		Very Low Risk					
		Not Analyzed					
3. *Cash activity*		High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					
4. *Other vulnerable factors*	Non-face-to-face	Available and Prominent					
		Available					
		Available but Limited					
		Not Available					
	Use of agents	High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					
	Anonymity (use)	Available					
		Not Available					
	Difficult to trace records	Records not available					
		Difficult/Time Consuming					
		Easy to trace					
	Existence of ML typologies	Exist and Significant					
		Exist					
		Exist but Limited					
		Does Not Exist					
		Exist and Significant					
		Exist					

Summary of the assessment of the Business/Profession:

Considering the assessment criteria and guidance, assess the inherent vulnerability variables associated with the assessed business/profession. For each business/profession, check (✓) the appropriate option in the table. Repeat this for each business/profession assessed.

			Business/Profession (Module 7.A) Product 1 (Module 7.B)	Product 2 (Module 7.B)	Product 3 (Module 7.B)	Product 4 (Module 7.B)	Product 5 (Module 7.B)
	Use in tax/fraud schemes	Exist but Limited					
		Does Not Exist					
	Other factor (specify)	High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					
	Other factor (specify)	High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					
		Not Analyzed					
	Other factor (specify)	High					
		Medium High					
		Medium					
		Medium Low					
		Low					
		Does Not Exist					

In case of a product-based assessment of a business/profession, please assess the inherent vulnerability variables associated with each product of the assessed business/profession. Repeat the assessment for all the products of assessed businesses/professions. Refer to Annex 2 for more details.

5. DESCRIPTION OF THE INTERMEDIATE VARIABLES

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

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

VARIABLE	DESCRIPTION
Inherent Vulnerability of a Particular Business/Profession **Product Inherent Vulnerability** **(Applicable for Product-Based Assessment Only)**	This variable assesses the susceptibility of a particular assessed business/profession as a whole or its product to money laundering solely based on key inherent factors of the business/profession or its products without taking into account its AML controls. An assessed business/profession or its product is inherently vulnerable when its characteristics render it open to abuse for money laundering. This relies on inherent vulnerability variables, namely: • *Total size/volume of the business/profession* (or product) • *Client base profile of the business/profession* (or product) • *Level of cash activity associated with the business/profession* (or product) • *Other vulnerable factors of the business/profession* (or product).
(Overall) Product Vulnerability **(Applicable for Product-Based Assessment only)**	This variable assesses the overall susceptibility of a particular business/profession's product to money laundering given its inherent vulnerability and the AML control mechanisms put in place to address that vulnerability. The more susceptible the product is, the more money laundering transactions can occur undetected. The overall product vulnerability depends on the: • *Inherent Vulnerability of the Product* (intermediate variable) • *Quality of AML Controls* (intermediate variable). **The ratings of all the product vulnerability assessments (of the assessed business/profession) determine the vulnerability of the assessed business/profession.**
Business/Profession Vulnerability	The overall vulnerability of the assessed business/profession is determined by its inherent vulnerabilities being assessed in conjunction with the quality of AML controls for the assessed business/profession.

ANNEX 1 – INSTRUCTIONS FOR USING THE EXCEL FILE

At this stage, the input variables have been assessed, and assigned a rating. These ratings now need to be entered into the Excel file. This Annex provides step-by-step instructions for using the Excel files (7.A/7.B) to assess the vulnerabilities of the businesses/professions in the DNFBP sector.

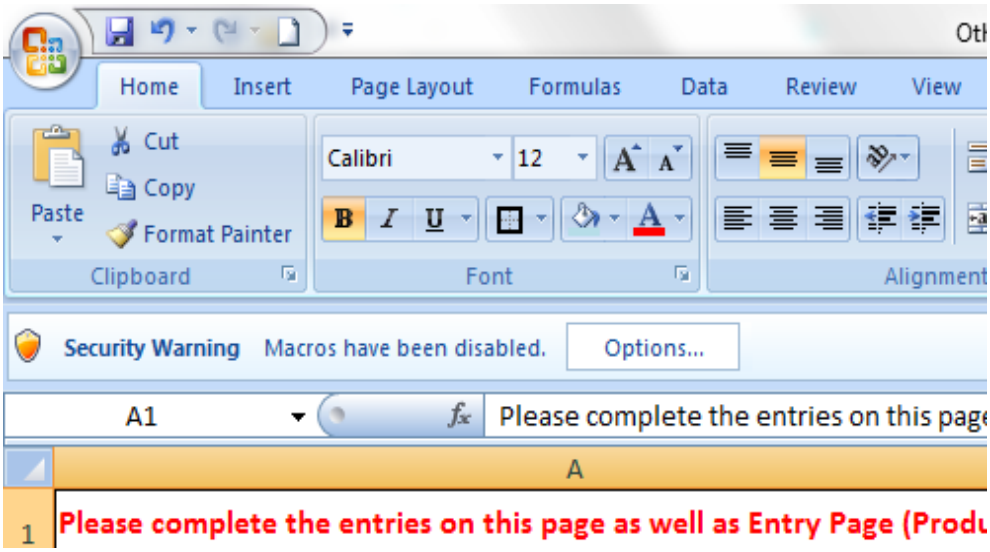
The WG should use Excel file 7.A if assessment is undertaken without detailed product assessment. In case of product-based assessment, use Excel file 7.B.

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

Step 1: Before you start

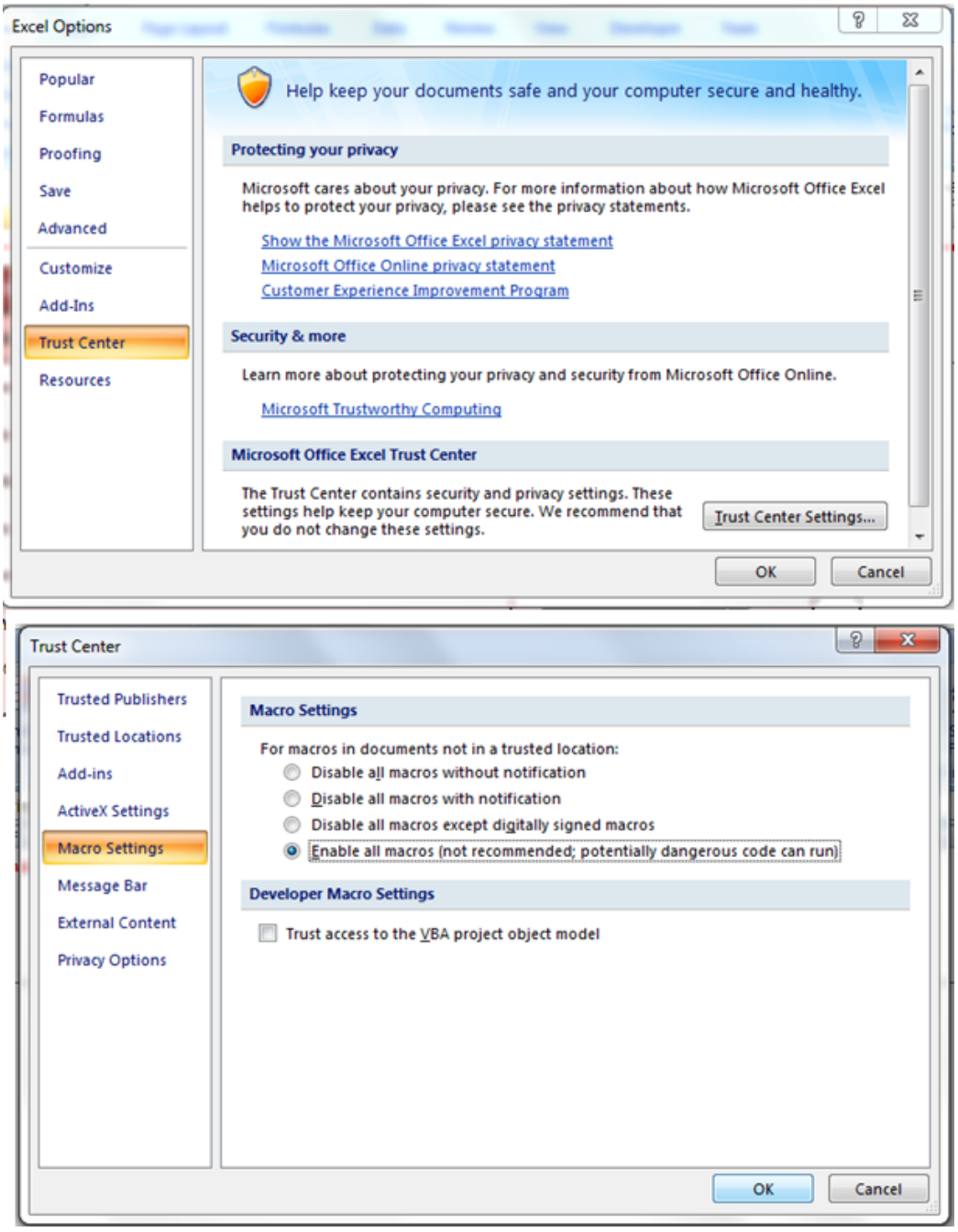
After opening the Excel file, first enable macros. A security warning will appear in the top left-hand corner of the first tab (Entry Page), warning you that macros are disabled – as shown in Figure 4.a. Click on the **Options** icon and select the **Enable this Content** option. Click **OK**, or (depending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

Figure 4.a: Macro security warning



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

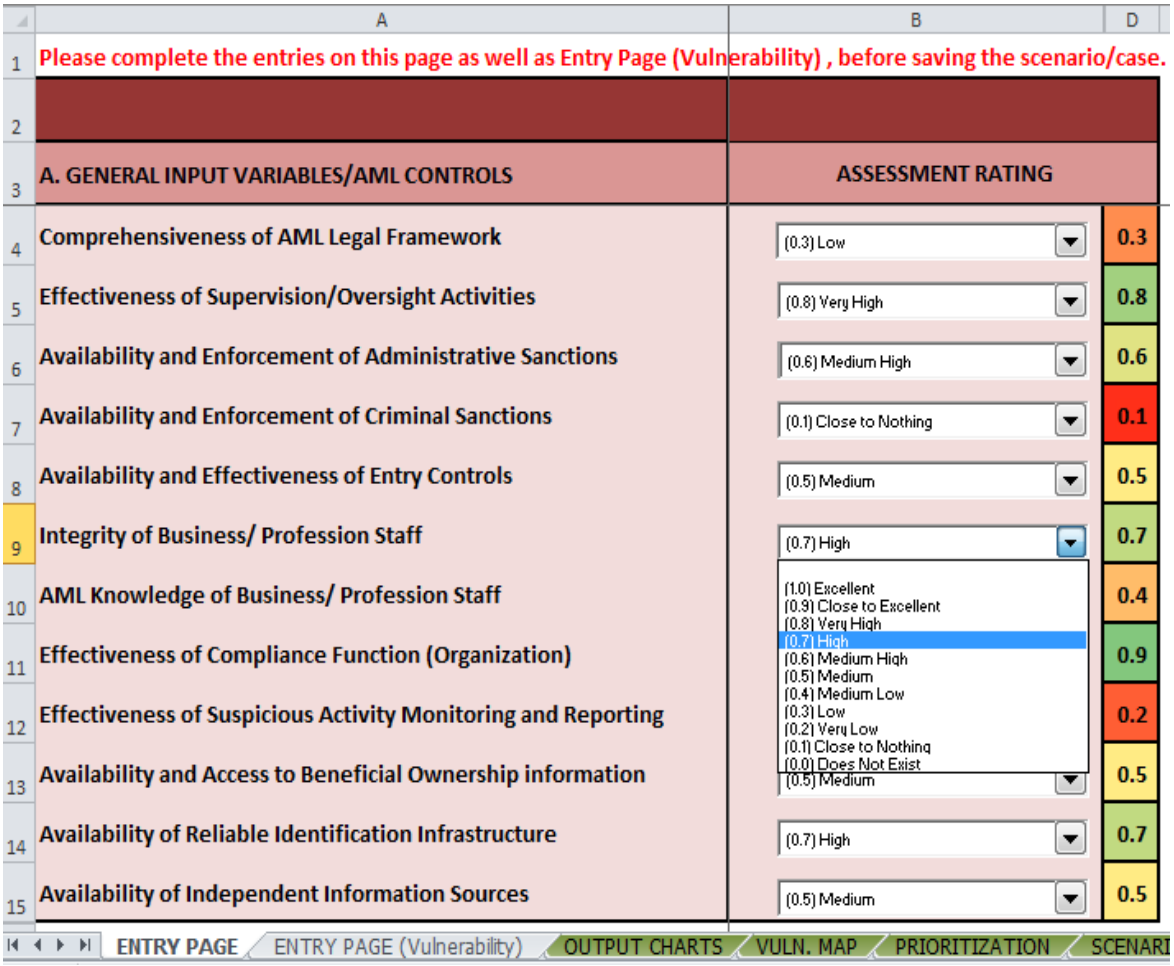
Figure 4.b: **Macro settings**



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

For each general input variable, select your chosen rating in the drop-down list. The options range from **(1.0) Excellent** to **(0.0) Does Not Exist**. Notice that higher assessment ratings for general input variables implies that the country has better AML controls in place, which will lead to a lower overall vulnerability for the assessed DNFBP business/profession. 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 (7.A and 7.B), the Entry (page) tab is similar.

Figure 5: **Entries for general input variables (in the Entry Page tab) (applicable to both Excel files, 7.A and 7.B)**



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

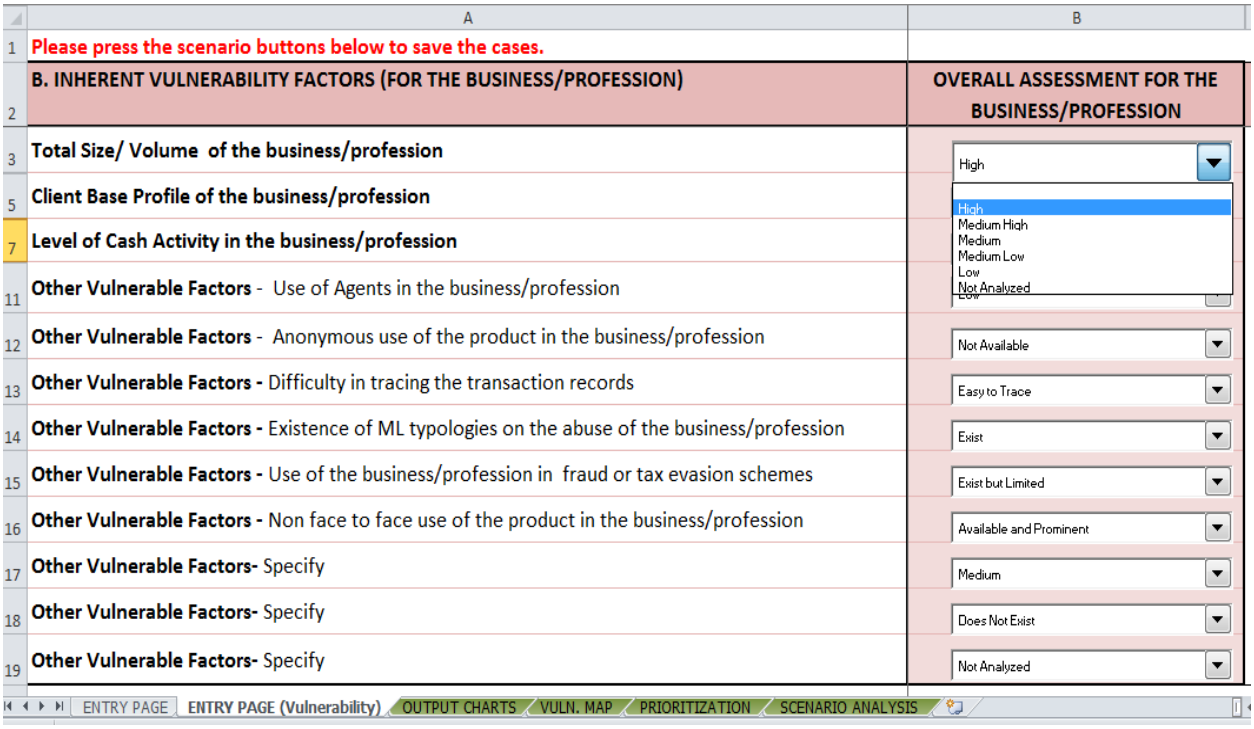
Bear in mind that the assessment of the general input variables is applicable to the assessed DNFBP business/profession as a whole, and will influence the vulnerabilities of all the firms and individuals operating within the assessed business/profession. In case of product-based assessment (Excel file 7.B), it will also influence the vulnerabilities of all the products offered by the firms and individuals operating within the assessed business/profession.

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 DNFBP business/profession are entered. During the assessment, you will decide which types of businesses/professions to include. Use separate Excel files for each type of DNFBP business/profession to be assessed.

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

Figure 6: Entries for inherent vulnerability variables (in the Entry Page (Vulnerability) tab), Excel File 7.A



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

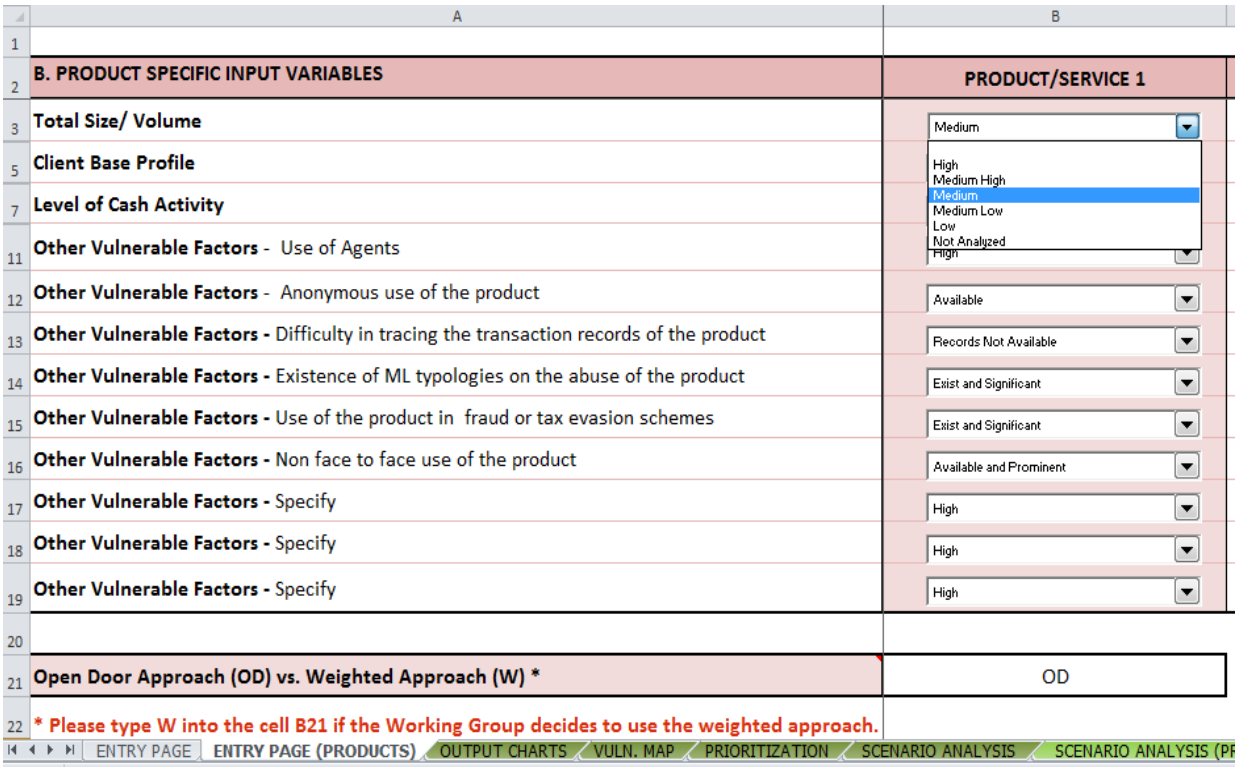
Step 3: Entries for inherent vulnerability variables (in the Entry Page (Products) tab) (applicable in case of product-based assessment, Excel File 7.B)

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

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 DNFBP business/profession (see Figure 7).

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

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



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

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

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

(2) **The Open Door Approach.** This approach calculates the vulnerability score of the assessed DNFBP business/profession, 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 7.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 DNFBP business/profession 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 7.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 7.A

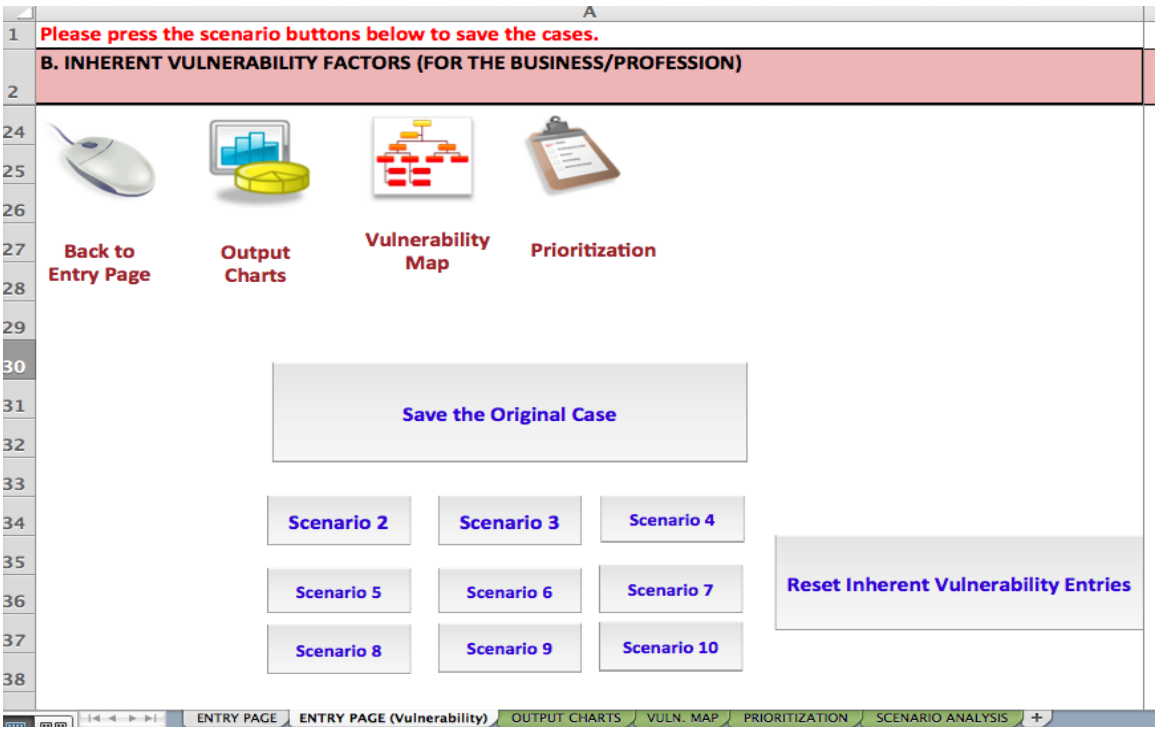
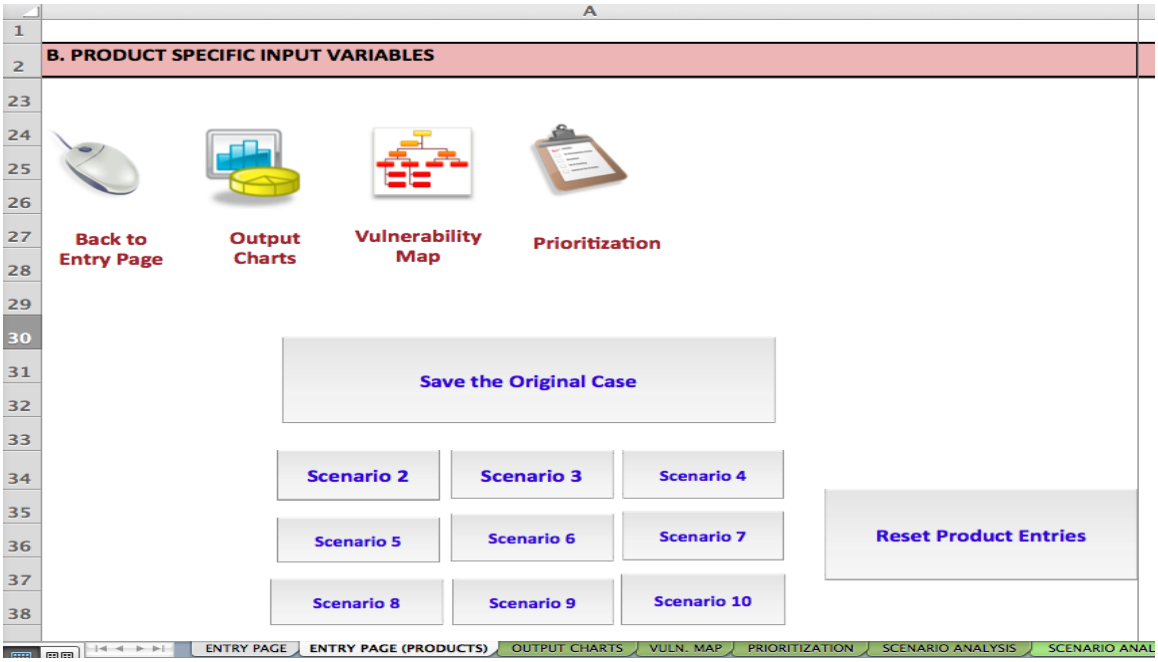


Figure 9: Icons on the Entry Page (Products) tab (applicable in case of product-based assessment, Excel File 7.B)



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:

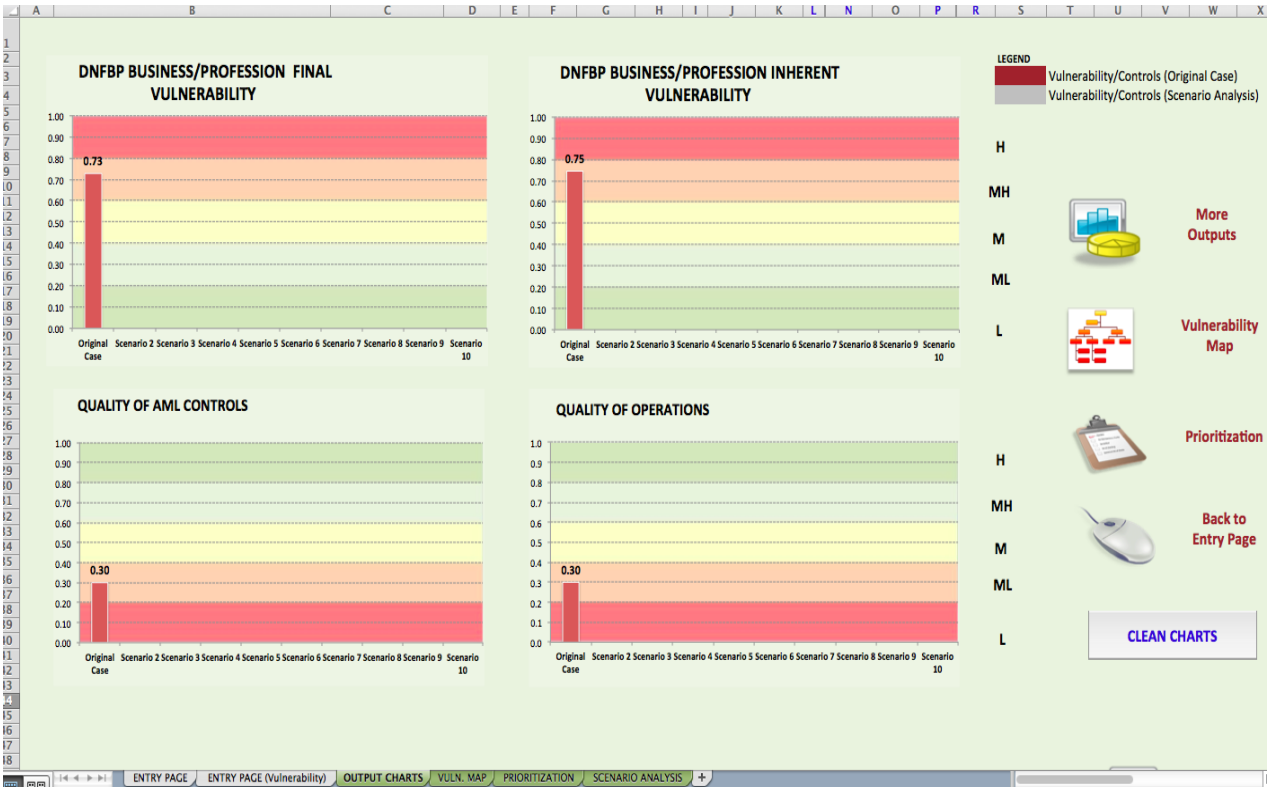
- Output Charts
- Vulnerability Map (Network Diagram)
- Prioritization.

(1) Output Charts tab

The Output Charts tab shows the final and inherent vulnerability score of the assessed DNFBP business/profession, 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 DNFBP business/profession does not take into account the impact of AML controls on the vulnerability of the business/profession. 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 DNFBP business/profession.

Figure 10: Output charts (Excel File 7.A)



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

Output Charts tab – For Product-Based Assessment (Excel File 7.B)

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

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

Figure 11.a: Output charts (applicable in case of product-based assessment, Excel File 7.B)

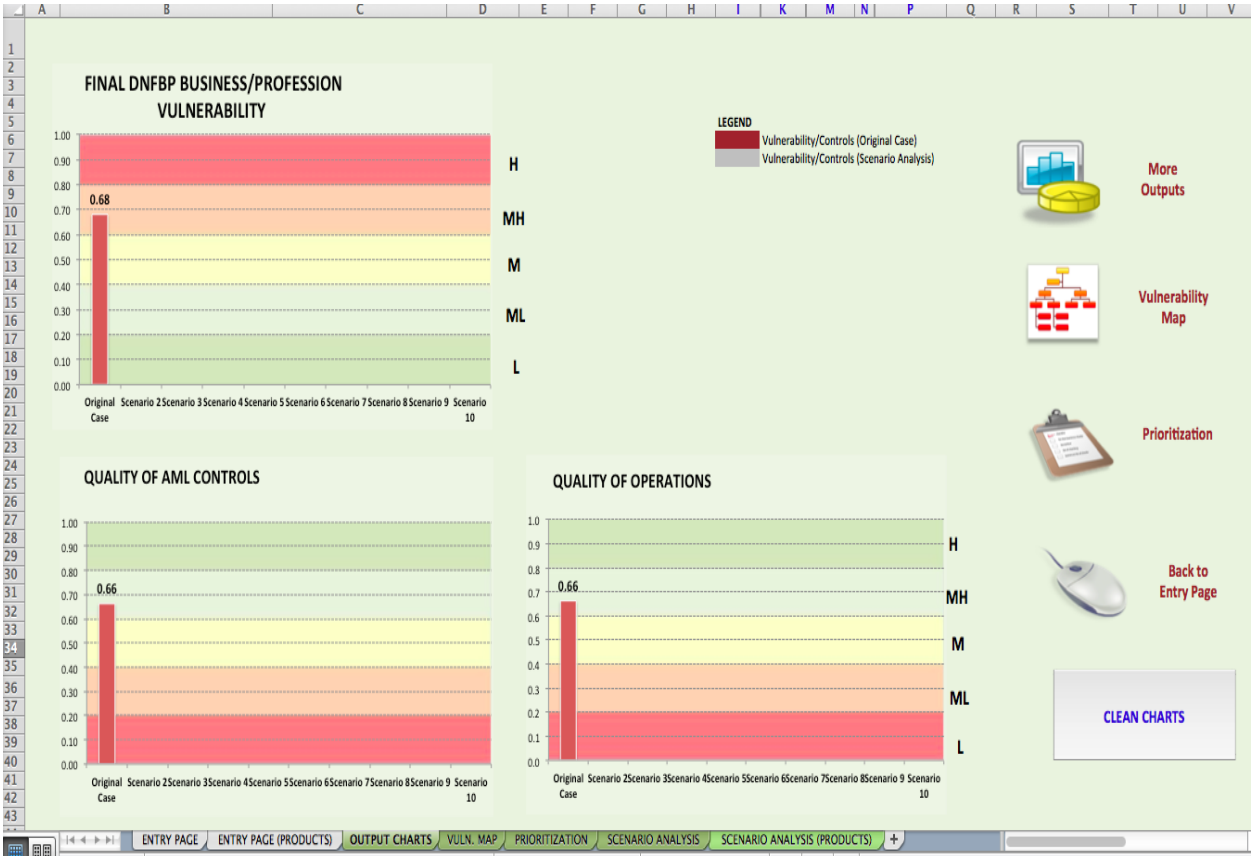
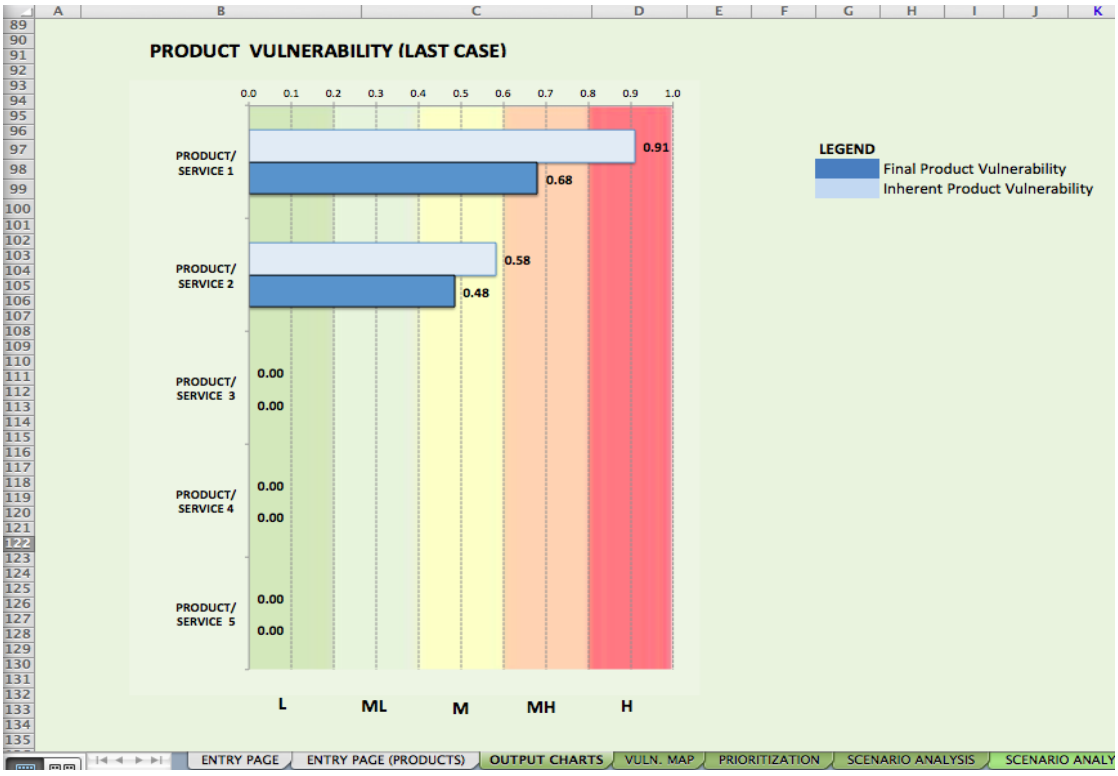


Figure 11.b: Product Vulnerability Output chart (applicable in case of product-based assessment, Excel File 7.B)



For both the product vulnerability chart and the final vulnerability of the assessed DNFBP business/profession chart, a higher score implies a higher vulnerability to ML. Similarly; a higher product vulnerability score increases the vulnerability score of the assessed DNFBP business/profession.

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

Applicable to both the Excel files (7.A and 7.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.

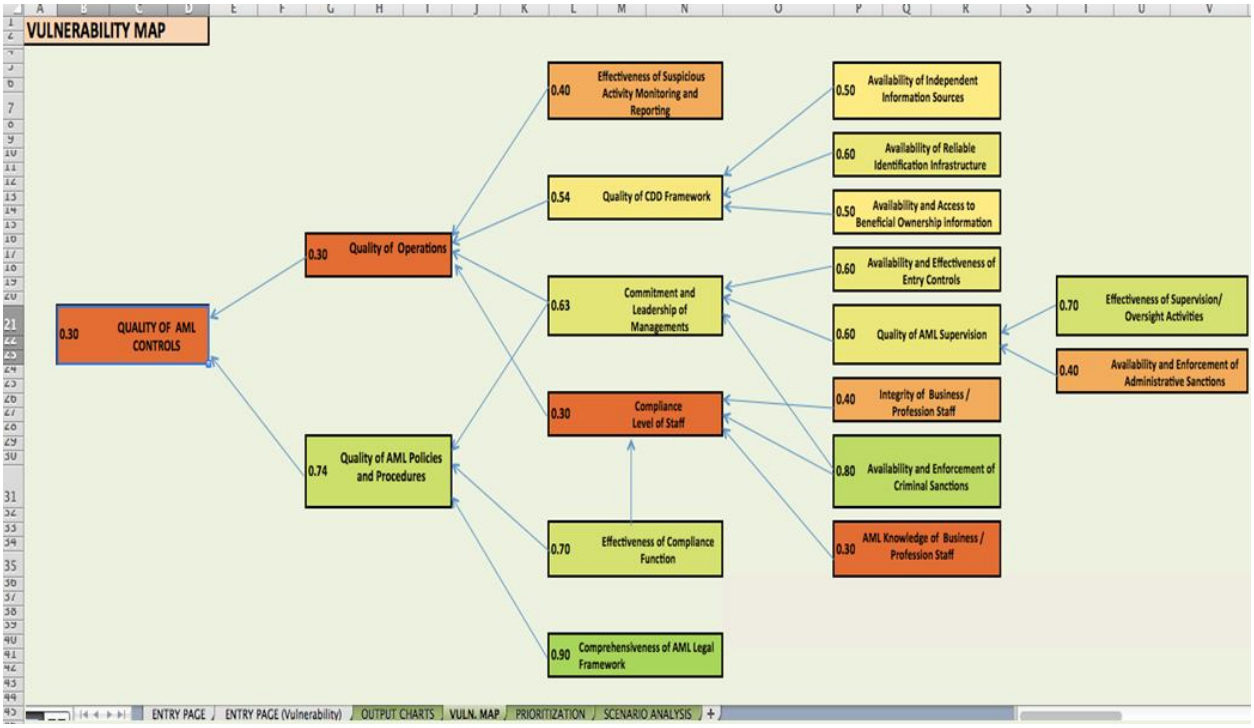
Please pay attention to the names and the colors of the inputs and outputs while interpreting the scores.

- 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 DNFBP business/profession, click on the **Vulnerability Map** icon on the Entry Page (Vulnerability) tab (as shown in Figure 8) or Entry Page (Products) tab (as shown in Figure 9) for product-based assessment – Excel file 7.B. This tab provides a visual summary of the assessment ratings of all the variables (see Figure 12). Note that the vulnerability map only shows the network diagram for the assigned assessment ratings of general input variables, and the corresponding assessment results of the intermediate variables, which affect the degree to which the assessed DNFBP business/profession 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 DNFBP business/profession (applicable only in case of product-based assessment – Excel file 7.B).

Figure 12: Vulnerability Map (applicable to both the Excel files, 7.A and 7.B)



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

Business/Profession Staff are the factors underlying Low *Compliance Level of Staff in* businesses/professions.

(3) Prioritization tab

A priority ranking can be generated to help guide relevant authorities to prioritize actions to strengthen AML controls within the assessed DNFBP business/profession. 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 7.B), Click on the **Prioritization** icon in the Entry Page (Products) tab (Figure 9) or in the Output Charts tab (Figure 11.a) to go to the Prioritization tab. The table in the Prioritization tab ranks the general input variables with respect to their impact on the AML controls and consequently the vulnerability of the assessed DNFBP business/profession (see Figure 13).

Figure 13: Prioritization table (applicable to both the Excel files, 7.A and 7.B)

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

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

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

Please note that the variable that has the lowest rating in the Entry Page tab may not have the highest priority rating in most cases. Priority rankings do not necessarily run parallel with the ratings in the Entry Page tab. Sometimes an item that is rated as medium may turn out to have the highest priority. Such results are fully consistent with the logic of the tool; as the assessment rating is just one of the four factors that have an impact on priority ranking. As previously explained, the other three factors are:

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

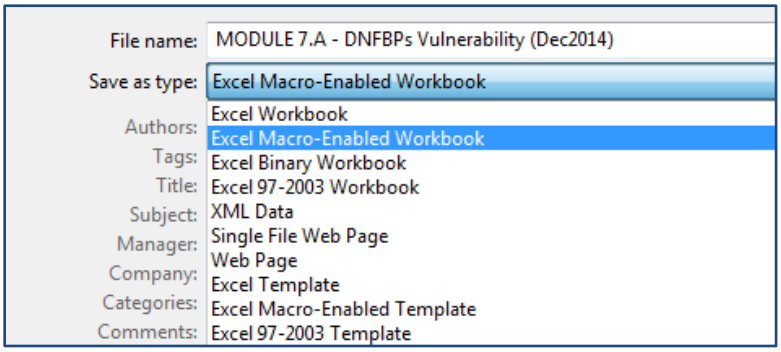
Applicable to product-based assessment (Excel File 7.B)

Whether an Open Door Approach or a Weighted Average Approach (or a combination of both approaches) is used to assess the vulnerability of the DNFBP business/profession, all the outputs and assessment results discussed in Step 5 will be the same for all three approaches. Only the final vulnerability of the assessed DNFBP business/profession 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 (Excel Files 7.A and 7.B)



Changing entries after the original case has been saved

If any changes have been made to the original case entries, remember to save those entries by clicking on the **Save the Original Case** icon on the Entry Page (Vulnerability) tab (see Figure 8) or Entry Page (Products) tab (see Figure 9) in case of product-based assessment – Excel file 7.B. The assessment outputs will not reflect the changes unless the entries have been saved.

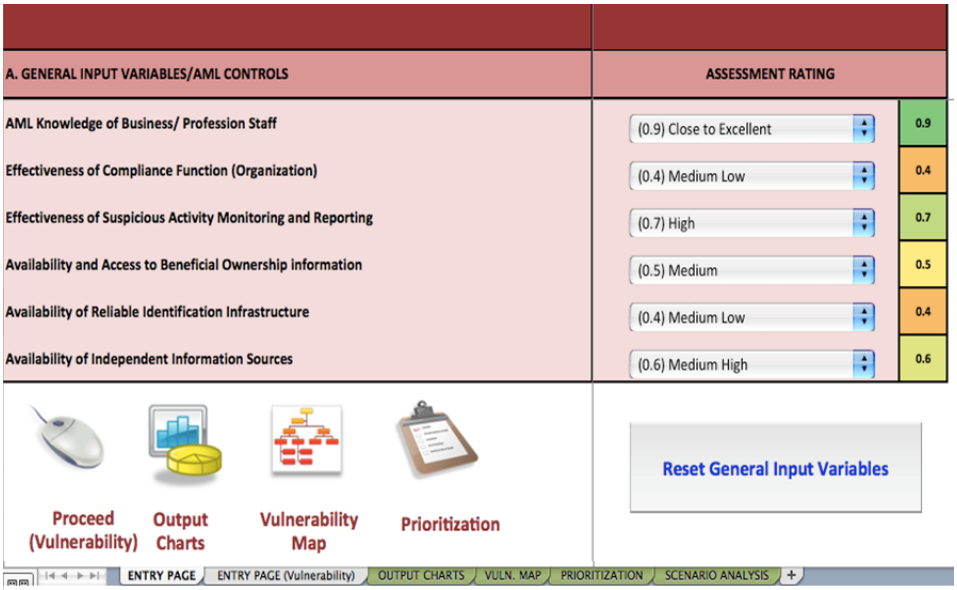
Erase all the entries and restart the process

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

Applicable to product-based assessment (Excel File 7.B)

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

Figure 15: Icons on the Entry Page tab– (applicable to both the Excel files, 7.A and 7.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 DNFBP business/profession 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 DNFBP business/profession, 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 7.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.

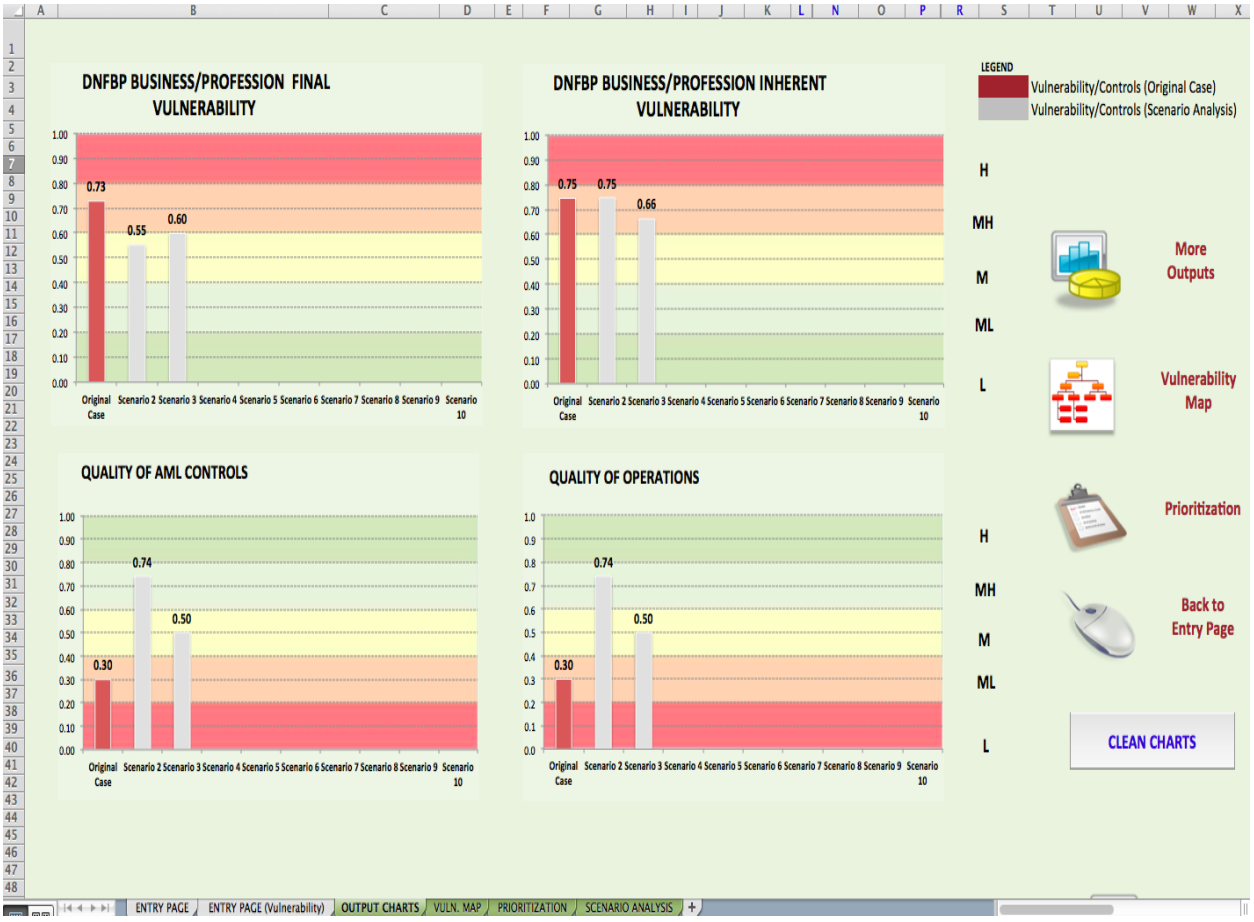
Instructions for using the scenario analysis option – Excel File 7.A

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 DNFBP

business/profession and the intermediate variables (such as *Quality of AML Controls* and *Quality of Operations*) are available for all the years (as shown in Figure 16).

Figure 16: Output charts – Scenario Analysis (Excel File 7.A)



***Instructions for using the scenario analysis option for* product-based assessment – Excel File 7.B**

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

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

Figure 17.a: Output charts – Scenario Analysis (Excel File 7.B)

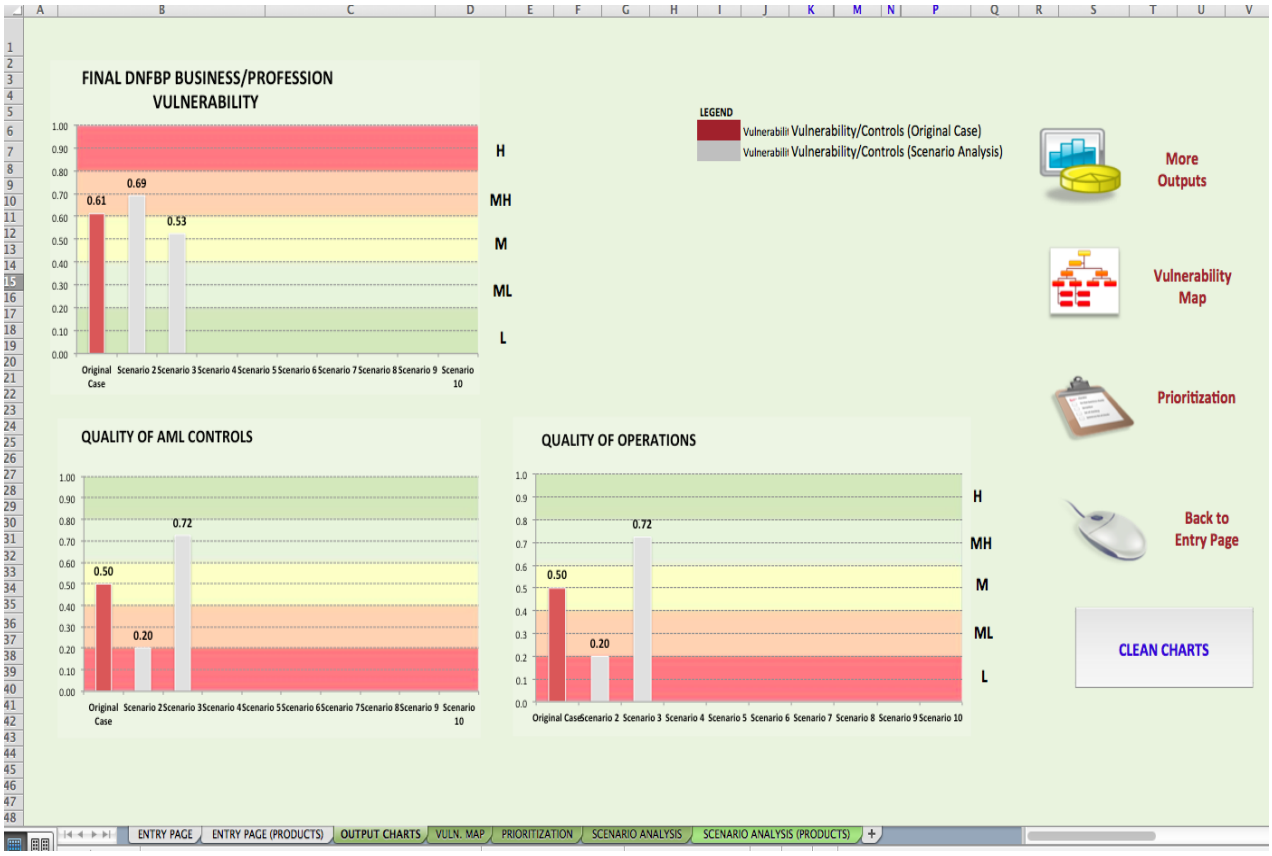
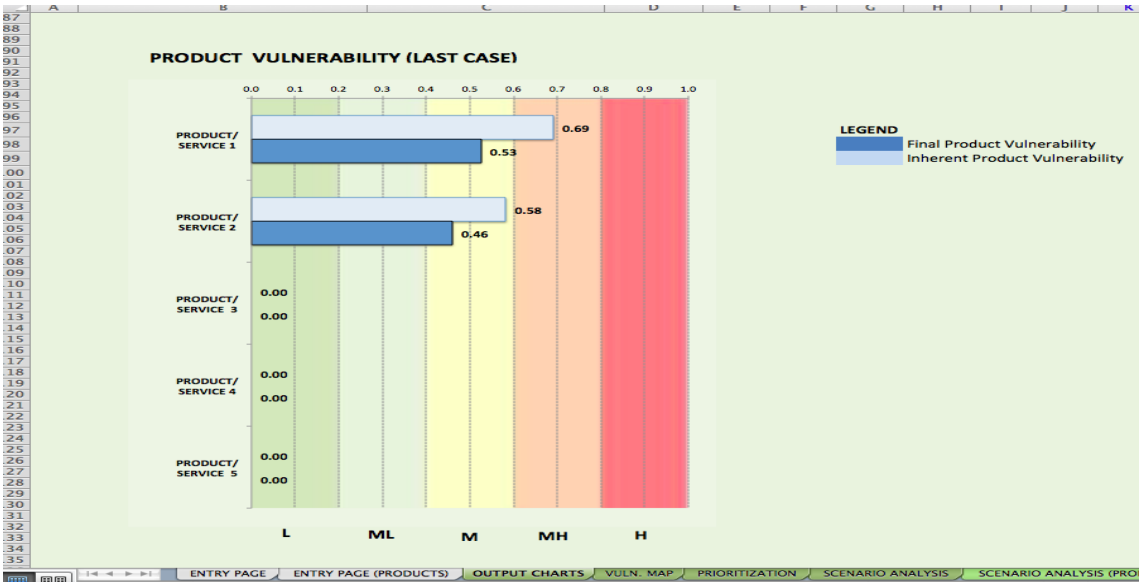


Figure 17.b: Product Vulnerability Output chart– Scenario Analysis (Excel File 7.B)



Scenario Analysis results – screen display (Excel Files 7.A and 7.B)

The Scenario Analysis tab provides the assessment results for the different years or scenarios (Figure 18). The Scenario Analysis tab shows the assigned assessment ratings for the general input variables, the assessment results for intermediate variables, the final and inherent vulnerability of the assessed DNFBP business/profession, 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 DNFBP business/profession originate, as well as the impact of policy actions on vulnerability, the combating ability/AML controls and the priority ranking of general input variables. The tables show how policy actions have an impact on the various components of vulnerability over a period of time, or in different scenarios.

Figure 18: Scenario Analysis tab (Excel Files 7.A and 7.B)

	A	C	D	E	F
1		Original Case	Scenario 2	Scenario 3	Scenario 4
2	INPUTS - GENERAL INPUT VARIABLES/AML CONTROLS				
3	Comprehensiveness of AML Legal Framework	0.9	0.9	0.5	
4	Effectiveness of Supervision/Oversight Activities	0.7	0.8	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	0.7	0.5	
8	Integrity of Business/ Profession Staff	0.4	0.9	0.5	
9	AML Knowledge of Business/ Profession Staff	0.3	0.9	0.5	
10	Effectiveness of Compliance Function (Organization)	0.7	0.6	0.5	
11	Effectiveness of Suspicious Activity Monitoring and Reporting	0.4	0.7	0.5	
12	Availability and Access to Beneficial Ownership information	0.5	0.5	0.5	
13	Availability of Reliable Identification Infrastructure	0.6	0.6	0.5	
14	Availability of Independent Information Sources	0.5	0.6	0.5	
15					
16					
17	OUTPUTS/ASSESSMENT RESULTS FOR INTERMEDIATE VARIABLES				
18	DNFBP BUSINESS/ PROFESSION FINAL VULNERABILITY	0.73	0.55	0.60	
19	DNFBP BUSINESS/ PROFESSION INHERENT VULNERABILITY	0.75	0.75	0.66	
20	QUALITY OF AML CONTROLS	0.30	0.74	0.50	
21	Quality of Operations	0.30	0.74	0.50	
22	Quality of AML Policies and Procedures	0.74	0.75	0.50	
23	Quality of CDD Framework	0.54	0.56	0.50	
24	Compliance Level of Staff	0.30	0.81	0.50	
25	Quality of AML Supervision	0.60	0.77	0.50	
26	Commitment and Leadership of Managements	0.63	0.75	0.50	
27					
28	PRIORITY RANKING FOR GENERAL INPUT VARIABLES/AML CONTROLS				
29	Comprehensiveness of AML Legal Framework			3	
30	Effectiveness of Supervision/Oversight Activities			2	
31	Availability and Enforcement of Administrative Sanctions	4		8	
32	Availability and Enforcement of Criminal Sanctions			9	
33	Availability and Effectiveness of Entry Controls	5		5	
34	Integrity of Business/ Profession Staff	2		6	
35	AML Knowledge of Business/ Profession Staff	1		1	
36	Effectiveness of Compliance Function (Organization)		1	3	
37	Effectiveness of Suspicious Activity Monitoring and Reporting	3		7	
38	Availability and Access to Beneficial Ownership information	7	3	11	
39	Availability of Reliable Identification Infrastructure	6	2	10	
40	Availability of Independent Information Sources	8	4	12	

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

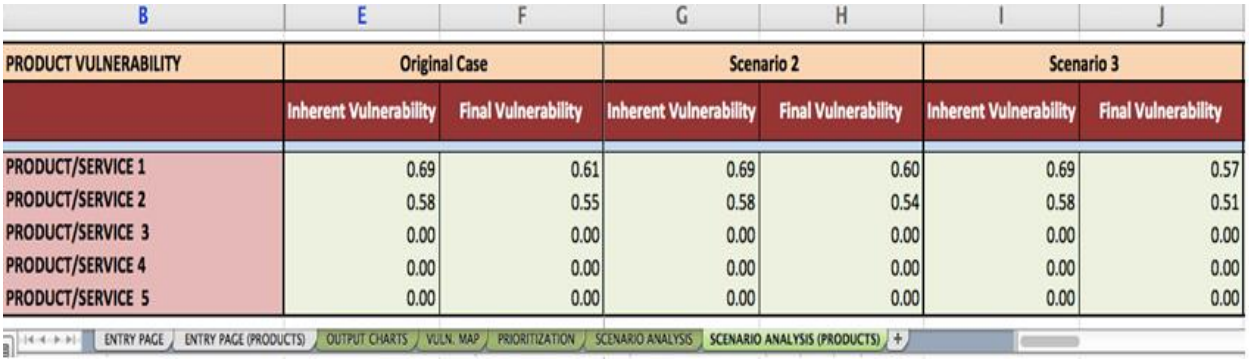
Scenario Analysis results–screen display for product-based assessment (Excel File 7.B)

The Scenario Analysis and Scenario Analysis (Products) tabs provide the assessment results for the different years or scenarios The Scenario Analysis tab shows the assigned assessment ratings for the general input variables, the assessment results for intermediate variables, the final vulnerability of the assessed DNFBP business/profession, and the priority rankings of the general input variables for the various years/scenarios (Figure 18).

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

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

Figure 19: Scenario Analysis (Products) tab (Excel File 7.B)



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

How to "unhide" the Weights tab

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

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

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

Figure 20: Weights tab (applicable to both the Excel files, 7.A and 7.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 BUSINESS/PROFESSION	WEIGHTS	PREREQUISITES
3	1. AML CONTROLS FOR THE BUSINESS/PROFESSION (Quality of AML Controls)	2	0
5	1.1. Quality of Operations	1	1
6	1.1.1. Quality of CDD Framework	1	0
7	1.1.1.1. Availability of Reliable Identification Infrastructure	3	1
8	1.1.1.2. Availability and Access to Beneficial Ownership information	3	0
9	1.1.1.3. Availability of Independent Information Sources	1	0
10	1.1.2. Effectiveness of Suspicious Activity Monitoring and Reporting	2	0
11	1.1.3. Compliance Level of Staff	3	1
12	1.1.3.1. Integrity of Business/ Profession Staff	2	0
13	1.1.3.2. AML Knowledge of Business/ Profession Staff	3	1
14	1.1.3.3. Effectiveness of Compliance Function	2	0
18	1.1.3.4. Availability and Enforcement of Criminal Sanctions	1	0
19	1.1.4. Commitment and Leadership of Managements	3	1
20	1.1.4.1. Availability and Effectiveness of Entry Controls	2	0
21	1.1.4.2 Quality of AML Supervision	4	0
22	1.1.4.2.1 Effectiveness of Supervision/Oversight Activities	2	1
23	1.1.4.2.2 Availability and Enforcement of Administrative Sanctions	1	0
24	1.1.4.3. Availability and Enforcement of Criminal Sanctions	1	0
25	1.2. Quality of AML Policies and Procedures	1	1
26	1.1.2.1. Comprehensiveness of AML Legal Framework	1	0
27	1.1.2.2. Commitment and Leadership of Managements	1	0
28	1.1.2.3. Effectiveness of Compliance Function	1	0
33	2. INHERENT VULNERABILITY OF THE BUSINESS/PROFESSION	3	1
34	2.1. Total Size/Volume	3	
36	2.2. Client Base Profile	3	
38	2.3. Level of Cash Activity	2	
42	2.4. Other Vulnerable Factors	3	

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

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

The defined 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 7.B)

The Working Group can decide to undertake a more detailed assessment of the products being offered by the assessed business/profession. This is to be decided on a needs basis as discussed in Section 2.1.

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

Why perform an assessment of certain products?

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

Module Structure (The Network)

As illustrated in Figure 22, the overall vulnerability of the business/profession is determined by the vulnerabilities of the various products assessed for the business/profession. This module assumes that product vulnerability can be measured by two main factors, which are determined by underlying sub-factors: (1) inherent vulnerability (of the product) and (2) quality of AML controls. "Product 1" is used as example in Figure 22. Similar assessments can be performed for other businesses/professions, and up to 5 products for each business/profession can be assessed.

Guidance for Assessment of Variables

For the assessment of AML control variables, refer to Section 4.1, where you can find assessment worksheets for AML control variables. The criteria for assessing AML control variables in product-based module are the same as the criteria for assessing the AML control variables for the specific business/profession. 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 business/profession. For assessment worksheets on inherent vulnerability variables, refer to Section 4.2.

Suggested list of products to assess

Please refer to Table 1 for a suggested list of products to assess.

Figure 22: Product-Based DNFBP Vulnerability Module Structure (Excel File 7.B)