WORLD BANK GROUP
Finance & Markets

NRA toolkit

NATIONAL RISK ASSESSMENT TOOL
GUIDANCE MANUAL

MODULE 1
MONEY LAUNDERING
THREAT ASSESSMENT

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 National ML Threat Assessment Module of the National ML/TF Risk Assessment Tool has been developed by a team that was led by Emiko Todoroki and included Kuntay Celik and Louis de Koker. The team thanks the staff and the management of the World Bank's Financial Market Stability and Integrity team for their significant contributions, which helped a lot in the improvement and the evolution of the module.

CONTENTS

Important reminders for the Working Group

- Base your assessments on group discussions to ensure the inclusion of a wide array of perspectives. All members of the Working Group should contribute to discussions as well as to the overall assessment, as the inclusion of all viewpoints and perspectives will contribute to a higher-quality report.
- Keep a record of the key arguments, findings, and conclusions of your discussions. These notes will be important when documenting the analysis and support for the conclusions and findings that will features in the final report. Assign a note-taker for this task.
- The quality of the output depends on the quality of the input. A defensive or unrealistic assessment will reduce the credibility of the assessment and will limit the benefits that the jurisdiction can derive from the assessment.
- During the assessment, please clearly identify any problems, weaknesses, or gaps in data and information collection. Such an approach will help you draw up the action plans for better data and information collection in the future.
- Support all your findings and conclusions with clear analysis and documented evidence, in order to demonstrate the basis for each of them.
- Prepare team reports on key findings and conclusions that are clearly documented with references to underlying sources. The team reports will become the building blocks of the National Risk Assessment report.

1. OBJECTIVES OF THE THREAT ASSESSMENT MODULE

The main objectives of this module are to:

- Identify money laundering threats and understand those threats in terms of type of predicate offense, origin, and sector
- Systematically collect data to assess money laundering threats
- Analyze cross-border threats from foreign jurisdictions.

The outcome of the threat assessment can be used to inform policy measures, support implementation efforts, and to improve the collection of data within the country.

2. UNDERSTANDING THE THREAT ASSESSMENT MODULE

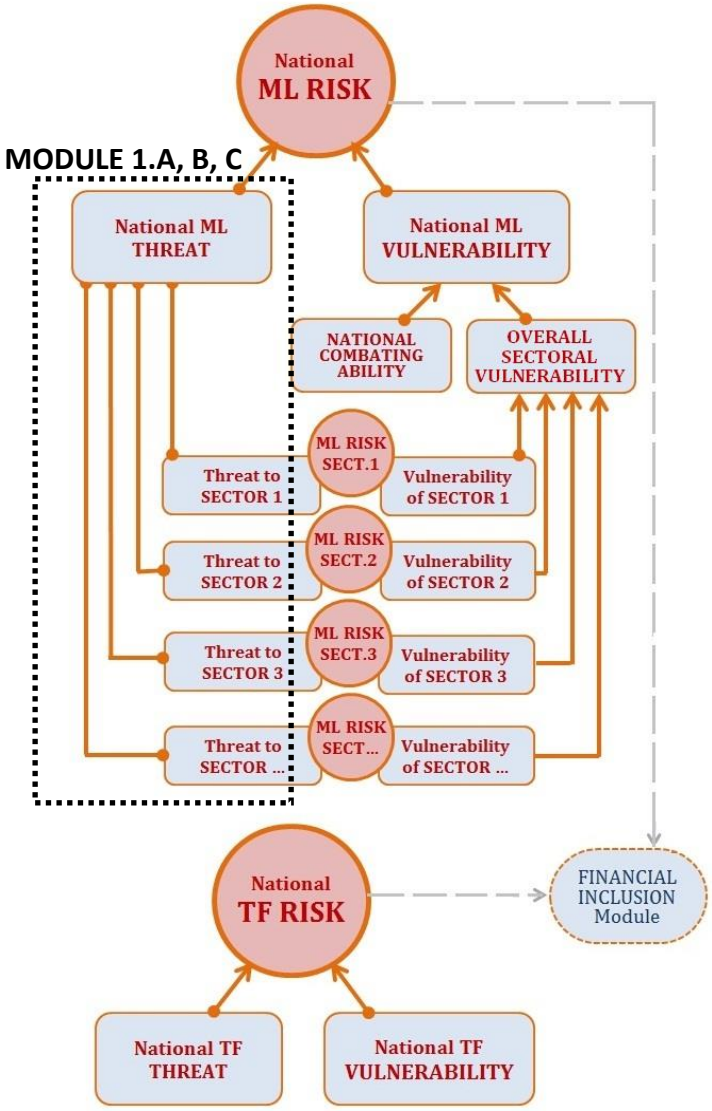
The module consists of the following three parts:

- ***Submodule 1.A.*** Focuses on assessing the predicate offenses that generate proceeds of crime, the total size of the proceeds of crime, and the sectors in which the proceeds of crime are invested and laundered.
- ***Submodule 1.B.*** Offers a framework for collecting data and information about the proceeds of crime and money laundering.
- ***Submodule 1.C.*** Focuses on assessing cross-border threats.

The primary vehicle of this module is Submodule 1.A, while Submodules 1.B and 1.C support Submodule 1.A by collecting inputs and ensuring their quality.

It is important to understand the module's place and function in the bigger picture of the National Risk Assessment Tool. As shown in Figure 1, threat and national vulnerability are the two main factors impacting the risk of money laundering at the national level. The threat module is based on the assumption that the money laundering threat is a function of "proceeds of crimes". Therefore, all submodules attempt to analyze generation, flows, and patterns of proceeds of crimes from different perspectives. At the end of the threat assessment, the country is expected to have a good understanding of money laundering threats to various sectors as well as the overall money laundering threat at national level.

Figure 1: ML Threat Assessment Module in the Big Picture of National Risk Assessment Tool



Where a country cannot supply full data on one of more of the required indicators, and/or lacks the ability to collect this data during the assessment, the module should use the quantitative and qualitative information that is available to complete the indicators as completely as possible. In such cases, strengthening existing frameworks, or establishing new frameworks for future data collection, should form a key element in the country's action plan.

Guidance on the period over which data needs to be considered is given in Section 4.

3. FLEXIBILITY OF THE MODULE

The module includes various tables as well as a large number of indicators. This gives assessors a wide range of options, which they may find useful in making the assessment. Having so many options may seem somewhat daunting, especially for jurisdictions that find it difficult to collect appropriate data in sufficient quantities. However, this apparent complexity is actually specious: compared to the other modules, this present module is less sophisticated, containing no macros. This means that it offers assessors a large measure of flexibility, making it easy for them to adapt it to their own situation. Assessors can skip indicators that are less relevant in the context of their country, and choose ones that are more meaningful, or more convenient, in terms of data and information collection.

4. DECIDING THE PERIOD FOR WHICH DATA NEEDS TO BE COLLECTED

The World Bank's National Risk Assessment methodology is based on informed, expert judgment. The purpose of data and information collection is to inform and facilitate sound judgment. This judgment is applied in determining the most appropriate period over which data information should be collected. For some indicators, data from the previous year 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.

Considering that in many countries anti-money laundering regimes have only recently been adopted, data collection periods will also depend on the availability of the data.

Money laundering cases usually take a long time to investigate, prosecute, and adjudicate. Furthermore, the number of money laundering convictions is often low in many jurisdictions. Working Group (WG) is therefore advised to use, if possible, data from the past ten years in their analysis. If this is not available, however, data from the past five years or past three years may be used instead. (See Table 1 for detailed guidance regarding different types of indicators.)

Table 1: Guidance on the data collection period

INDICATORS	DATA COLLECTION PERIOD
Quantitative indicators of money laundering threats	Depending on the availability of data, ten, five or three years.
Qualitative indicators of money laundering threats	This is mostly qualitative information and does not require a strict timeframe. The most meaningful information is the most recent information, so try to obtain as much information from the past five years as possible.
Quantitative indicators of overall financial flows	The indicators are flow variables, which consist of annual amounts. Obtain information from the past five years. These statistics are usually published by central banks on a quarterly basis. Use the most recent data at the time of the assessment.

Since this is not a statistical model, there are no strict conditions on having identical data collection periods that need to be applied to all indicators. Using different data collection periods in different sections is not problematic for the overall model. The indicators are analyzed per jurisdiction, and the present situation within the jurisdiction is assessed on that basis. However, it is important that there is consistency across the rows and columns relating to a given indicator. For example, if one wishes to compare the amount of mutual legal assistance offered across various jurisdictions, then it is necessary that the data used was collected in the jurisdictions over the same time period (e.g., five years).

5. SOURCES OF DATA AND INFORMATION

The following table provides guidance about which data and information sources can be used for completing the cross-border threat assessment.

Table 2: Guidance on data and information sources

INDICATORS	DATA AND INFORMATION SOURCES
Quantitative indicators of money laundering threats	• Judicial system database • National statistics agency • Prosecutor's Office database • Law enforcement database • Financial Intelligence Unit database • Anti-corruption agency database • Agency for managing seized and confiscated assets • Tax authority • Customs authority • Research reports and academic studies
Qualitative indicators of money laundering threats	• Intelligence • Reports by government agencies • Academic studies and publications • Publications by international organizations • Publications by nonprofit organizations • Open sources (e.g., Internet, and public news) • Surveys with focus groups or the general public • Interviews with focus groups or experts
Quantitative indicators of financial inflows and outflows	• Central bank • National statistics agency • Commercial databases (such as SWIFT) • Financial institutions • Financial supervision authorities

6. SUBMODULE 1.A – THREAT ASSESSMENT MODULE

6.1 Introduction

The Excel file for Threat Assessment Submodule 1.A consists of four separate tabs that contain individual tables for:

- Predicate offense breakdown
- Origin breakdown
- Sector breakdown
- Overall assessment.

Detailed information for each tab is provided in the following sections.

6.2 Predicate Offense Breakdown

The tab for predicate offenses is where statistics and information regarding proceeds-generating crimes and money laundering cases committed within the jurisdiction are collected and analyzed. The purpose of this analysis is (1) to help establish which type of predicate offense is most prevalent in the jurisdiction, and (2) to estimate the size of the proceeds generated by these crimes.

Column A: List the most relevant predicate offenses for money laundering in the jurisdiction

The WG should compile a list of those predicate offenses that are considered most relevant, on the basis of the legislation and prevalent criminal behavior patterns within the jurisdiction. The WG should take into consideration all proceeds-generating criminal offenses that are predicate offenses under the jurisdiction's legislation. Predicate offenses may include fraud, embezzlement, bribery, drugs trafficking, human trafficking, illegal logging, and profit-making environmental crime. The list may be compiled on the basis of expert opinions and other available sources of information. Predicate offenses that are obviously irrelevant or insignificant in the country context may be excluded from this analysis. In deciding which predicate offenses are most prominent in the jurisdiction, account may be taken of the input to the brainstorming sessions held at the beginning of the first workshop.

The WG is advised to focus on proceeds-generating crimes and to distinguish them from other crimes that may be categorized as similar. For example, within the drug offenses category, focus on the drug offenses that generally generate more substantial proceeds, such as drug trafficking. If an assessor combines all the drug-related crimes (including possession of small amounts) in the same row, the statistics may be misleading. It may therefore be better to omit cases related to possession, or at least to assess them as a separate category. The same approach should be taken when dealing with other, similarly broad categories of crime, such as arms smuggling as opposed to the illegal possession of firearms. In this example, the first crime is a proceeds-generating crime, while the second is not. The first category is therefore the more meaningful category for the purposes of this assessment.

Depending on the criminal environment in the country, some categories of crime may require further breakdown. For example, rather than recording all fraud crimes altogether, the WG may need to distinguish internet fraud, banking fraud, and insurance fraud from other types of fraud. Additional rows can be added by the WG, as required, to capture these various distinctions.

Columns B–G: Collect enforcement data about the predicate offenses

These columns collate enforcement data from law enforcement, prosecutorial, and judicial authorities concerning predicate offenses. The WG should insert data about the number of cases that have been detected, investigated and that have resulted in a prosecution and conviction, as well as the amounts of proceeds seized, frozen, and/or confiscated.

When recording the number of investigated and prosecuted cases, enter the number of cases rather than the number of defendants. In terms of convictions, there are two separate columns in which to enter data: one for the number of convictions, and one for the number of persons convicted. Please try to fill both columns as fully as possible.

If there are any proceeds of crime that are frozen or confiscated based on the general provisions of the penal code or other laws (without money laundering charges), please record these in Columns F and G.

The template deliberately distinguishes between the analysis of predicate offenses and that of money laundering cases. The number of the money laundering cases may be relatively few in some jurisdictions, especially if those jurisdictions have only recently criminalized money laundering. In such cases, analysis of predicate offenses may still provide valid insight into the proceeds of crime, and therefore the money laundering risk. For other jurisdictions, this analysis will help contribute to a better understanding of what proportion of the total proceeds of crimes are being laundered, or are suspected of being laundered.

Columns H–N: Analyze all detected money laundering cases according to underlying predicate offenses

For example, if the first row is focusing on drug trafficking, Columns B to G will capture the numbers related to drug trafficking cases. Apart from this, Columns H to N should capture the numbers related to the money laundering cases, in which the predicate offense was drug trafficking. A country may have hundreds of drug trafficking cases, but only a few money laundering cases linked to drug trafficking. This comparison can make useful input regarding the effectiveness of the legal actions against money laundering.

If the country is not able to identify the exact predicate offenses underlying some money laundering cases, and therefore cannot link them to any of the predicate offense rows in the table, please record them in the "Money Laundering Cases with Unclear/Unidentified Predicate Offense" row at the bottom of the table.

Column O: Capture other information about predicate offenses and their proceeds

The WG should capture information in this column from other sources of information beyond law enforcement data. Sources could include reports from the Auditor General, Special Commissions, academic reports and studies, or some qualitative information such as intelligence, public information, or surveys or interviews with relevant focus groups. The on-the-spot expert survey of the first workshop may help to identify useful sources of information.

Column P: Capture information from FATF Mutual Evaluation Reports

Findings from the Mutual Evaluation Reports of the Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRBs) can be included here, especially when they provide information on the prevalence and details of predicate offenses and money laundering.

Column Q: Estimate undetected and unrecorded predicate offenses and their proceeds

Enforcement data do not capture all crimes and criminal proceeds in a jurisdiction exhaustively. It is therefore necessary to attempt to estimate those predicate offenses and proceeds that are not detected or recorded (the "hidden part of the iceberg"). The WG should capture the estimates for the relative size of detected and recorded proceeds of crime (as filed in Columns B to H) to the total estimated proceeds of crime for each of the listed predicate offenses.

The estimates can be recorded in the Excel template in various ways. For example:

- *"The detected proceeds are estimated to represent X percent of the total criminal proceeds for* [the relevant predicate offense].*"*
- *"The undetected proceeds from* [the predicate offense] *are estimated to be at least X times the detected amounts."*
- *"The undetected proceeds from* [the predicate offense] *are estimated to be lower/equal to/higher than the detected amounts."*

Please note: This column is *not* for secondary or optional inputs. It aims to describe other substantial information that is not reflected in the quantitative enforcement data and is therefore a significant column in the table.

Columns R–V: Assess the money laundering threat per predicate offense

Based on the data and information in the table, the WG needs to make a judgment about the money laundering threat arising from each predicate offense.

When making an assessment, the WG should focus on the proceeds of crime and the money laundering aspects of predicate offenses. In many countries, enforcement data will often reveal theft and similar petty crimes to be the most prevalent criminal offenses. However, such offenses are less relevant for a money laundering analysis, as the average amount and value of the proceeds of such offenses will probably be low and the proceeds will be spent rather than laundered. The extent of money laundering for each predicate offense should be the decisive factor in conducting the assessment. The involvement of organized crime groups should be considered when assessing the money laundering threat that arises from a particular category of criminal offenses.

The threat can be assessed to be from "low" to "high".

6.3 Origin Breakdown

The breakdown in terms of origin aims is designed to facilitate the identification of patterns regarding the jurisdiction of origin of proceeds of crimes. This may be particularly relevant in cases when the predicate offense to money laundering was committed in a foreign jurisdiction.

There are four possible scenarios:

1. The predicate offense is committed in a foreign jurisdiction, but the proceeds are laundered in the home jurisdiction.
2. The predicate offense is committed in the home jurisdiction, and the proceeds of crimes are also laundered there. Even if the proceeds are later transferred to other jurisdictions, some initial acts of the laundering offense will have occurred in the home jurisdiction.

3. The proceeds that are laundered in the home jurisdiction are generated by predicate offenses committed in both the home jurisdiction and in foreign jurisdiction(s).
4. The origin of the proceeds of crimes cannot be identified; it is therefore not clear whether they are generated from within the home jurisdiction or in foreign jurisdiction(s).

In jurisdictions with developed financial markets, diverse financial instruments, and attractive investment opportunities, the external threat[1] may exceed the internal threat.[2] On the other hand, jurisdictions with closed economies, moderately developed financial markets, and/or limited integration into the global financial system are likely to be less attractive to foreign proceeds of crime.

The "Module 1.C – Cross-border Threat Assessment" Excel file is also linked with this table. While this table aims to identify the origins of the detected money laundering cases, Module 1.C attempts to identify cross-border threats by using a broader range of indicators. Nevertheless, the data in this template can still usefully serve as input to Module 1.C.

6.4 Sector Breakdown

The Sector Breakdown tab in the Excel file facilitates the analysis of the money laundering threat as it materializes within different sectors. While the previous two templates focus on the amount of proceeds of crime generated through predicate offenses, the present section enables the analysis of how the proceeds are being invested and laundered and in what sectors.

The possibility of accurate analysis depends on there being information and data relating to money laundering cases. A country will be able to analyze the sector breakdown, if it is able to complete the data collection template (Module 1.B). The rows that relate to the sectors being abused in each money-laundering case (in Module 1.B) are central as the input to this tab. Identifying these data helps determine those sectors, which are possibly being used to launder funds. On the basis of Module 1.B, the WG will then be able to establish the percentage of cases involving particular sectors.

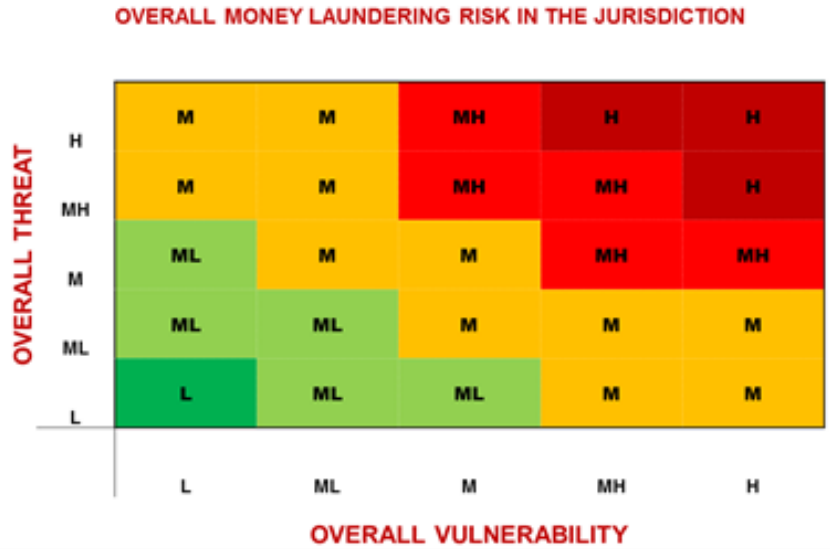
As in the case of enforcement data, in order for the analysis to be comprehensive, this analysis should attempt to include cases that have not been detected or reported.

The first step in the assessment is to adjust the list of sectors to reflect the most relevant sectors in the jurisdiction. The sectors that are listed by default (in the Excel file) can be amended and are only intended to serve as preliminary suggestions. The WG should check with the other sub-work groups to make sure that the list of sectors in this module captures all the sectors being assessed in the other modules. The list of the sectors in this module should be identical to the list of sectors in the modules that assess vulnerability (Module 2 "National Vulnerability"). If the sub-WG for Module 2 is assessing the vulnerabilities of fifteen different sectors, the same fifteen sectors should be analyzed in this module. Make sure that all categories of financial institution and designated non-financial businesses are also included.

As the money laundering risk is determined by threat and vulnerability, the tool uses the following "heat map" to identify the overall money laundering risk. It works by combining the outcome of this module for the overall threat with the outcome of the module for overall vulnerability.

1. Occurrence of laundering of proceeds of offenses committed abroad.
2. Occurrence of laundering of proceeds from offenses committed domestically.

Figure 1: Overall money laundering risk as a combination of threat and vulnerability



By analyzing both the money laundering threat and the vulnerability by sector, the risk of money laundering can be established for each sector.

Completing the sector threat assessment will enable the WG to assess the "risk" at sector level.

For example, if the country has a threat and vulnerability assessment for the real estate sector, the WG can make an assessment of the money laundering risk in the real estate sector, using the same heat map that is used for the overall risk assessment. The WG is advised to discuss in its written report first the risk of money laundering per sector (as a combination of identified threat and vulnerability levels), and then support its findings relating to risk by an analysis on both the threats and vulnerabilities of the sector.

Such an assessment is possible only if the country is able to make a sector threat assessment using the data collection template (Module 1.B) and the sector breakdown table. When assessing the sector breakdown, be cautious about using suspicious transaction data, and try to rely as far as possible on data from detected money laundering cases. The results of the discussion and on-the-spot surveys during the first session of the workshop may be a useful input in the assessment.

6.5 Overall Assessment

Upon completion of the tables, the WG should now have significant information that will enable it to make an overall assessment of the internal, external, sector, and overall threat. This page contains some cross-references to the parts of the assessment. These cross-references will make it possible to develop an assessment of the overall threat. The result will be one of the main inputs to establishing the overall money laundering risk of the jurisdiction.

This tab represents the final stage of the money laundering threat assessment. It is therefore the last threat template to be filled in. Key input needed here is from the Cross-border Threat Assessment (Module 1.C). The assessors should therefore return to this tab after completing all other parts of Module 1, including Modules 1.B and 1.C.

7. SUBMODULE 1.B – CASE BASED DATA COLLECTION MODULE

7.1 Introduction

The aim of Submodule 1.B is to support the collection of detailed information from available money laundering cases. This collates the data and information in a systematic database. Having such data and information allows systematic analysis regarding trends and patterns of money laundering in the jurisdiction. An ongoing systematic collection of data will also contribute significantly to the monitoring and future analysis of money laundering trends. The higher the number of cases from which information can be extracted, the more meaningful the analysis will be, especially from a statistical point of view. But even if there are only a few cases, and the initial analysis will therefore have only limited statistical value, the submodule should still be completed. This is because it will provide the jurisdiction with a starting point for comprehensive data collection on an ongoing basis.

7.2 Compiling Data from Money Laundering Cases

The first column covers a list of the detailed information to be collected from an individual money laundering case. This list may be modified by (for example) changing the names, expanding the list for a more detailed data collection process, or deciding to collect only some of the most significant indicators).

Most jurisdictions do not have this kind of data readily available. To find the data, it may be necessary to review the files of individual cases. The table is for collecting statistical data; confidential information from cases does not need to be recorded. Authorities can thus choose to address any confidentiality issues by making reference to cases through numbers or other labels. If a jurisdiction does not have any money laundering cases, the WG should record this fact here.

The table is designed to capture (respectively) those cases that resulted in a conviction, those that went to prosecution but did not result in a conviction, and those that were merely investigated. The most reliable information will typically come from those cases, which resulted in a conviction, as the money-laundering component has been proven in them. Data from suspicious transaction reports (unless they turn into an investigation) are not considered in this table, as they may not provide reliable information.

Assessors should not feel discouraged if they have not been able to fully complete the template. The objective of this submodule is broader than the current National Risk Assessment and aims to guide the jurisdiction in establishing a systematic and strong framework for future data collection. If the jurisdiction does not yet have detailed data collection procedures in place, establishment of a data collection framework should be included in the action plan. By initiating this data collection at the time of the first National Risk Assessment, considerably more data will be collected in the next National Risk Assessment. This will support the jurisdiction in conducting much more robust risk assessments in the future. Such a database can also serve as a valuable data source for research and policy purposes.

8. SUBMODULE 1.C – CROSS-BORDER THREAT ASSESSMENT MODULE

8.1 Introduction

Submodule C aims to support the assessment of the cross-border laundering threat to the jurisdiction. The cross-border threat relates (a) to the laundering of proceeds of crime committed outside of the jurisdiction and (b) to the laundering of domestically generated proceeds of crime in other jurisdictions. Completion of this submodule may show up patterns of abuse of the jurisdiction – as a destination or jurisdiction of origin for incoming illicit funds, or as a transit route. Data on money laundering cases and typologies must first be compiled and sorted by country/jurisdiction. Then, data on the economic relations with other jurisdictions (specifically on the financial inflows and outflows from and to other jurisdictions) must be gathered. The WG should discuss and determine the potential cross-border threat per jurisdiction by contrasting these two sets of data.

8.2 Cross-border Threat: Data on Money Laundering Cases and Typologies by Jurisdiction

Selection of jurisdictions for the corridors to be assessed (Column A)

Column A is for listing the relevant jurisdictions. These are the corridors that will be assessed. Each row needs to be allocated to one other jurisdiction. The data and information regarding that specific jurisdiction needs to be completed in relevant cells of the same row.

Depending on the country context, the WG should examine the corridors with at least five to ten jurisdictions that have the most significant criminal, cultural, economic, or financial links with the assessed jurisdiction (see recommended criteria below on how to determine this list of countries). There is no limit to the number of jurisdictions that may be examined: in fact, the more jurisdictions examined the better, as it makes the assessment more comprehensive.

The list of jurisdictions is not meant to be static. It may need modification depending on the indications of collected data. The following steps are recommended for selecting the jurisdictions to be included in the assessment. These are only indications – always use your common sense, and if you feel some countries do not belong on the list, or others do, amend as necessary.

Table 3: Steps to determine the jurisdictions to be included in the cross-border threat analysis

Step	Description of suggested procedure
1	Start with the jurisdictions that were identified during the general discussion and brainstorming session on the first day of the workshop.
2	Analyze the ML convictions and identify the top ten jurisdictions (or as many as relevant) that appear in these cases. Compare this list with your list in Step 1, and expand the list so as to include these ten jurisdictions.
3	Analyze the data of outgoing mutual legal assistance requests. Identify the top ten jurisdictions (or as many as relevant) and compare them with your list in Step 2. If there are new jurisdictions that are not already in your list, expand the list to include them.
4	Analyze the data of incoming mutual legal assistance requests. Identify the top ten jurisdictions (or as many as relevant) and compare them with the list in Step 3. Repeat as above.
5	If data on financial inflows (as set out in Submodule 1.C) are available, identify the top five (or as many as relevant) jurisdictions and repeat as above.
6	If data on the financial outflows (as set out in Submodule 1.C) are available, identify the top five (or as many as relevant) jurisdictions and repeat as above.
7	If the home jurisdiction has a significant Trust and Company Service Provision sector, identify the top five origin jurisdictions (or as many as relevant) of the clients. Repeat as above.

The WG is encouraged to focus on the most relevant jurisdictions (likely to be between five and fifteen). An overlap is likely between the jurisdictions in the various steps described above. Should one of the other indicators prove to be more meaningful for selecting the jurisdictions, the steps should be modified.

Please note that for these seven items, the data need to be as complete as possible. For example, to ensure that the top ten jurisdictions can be identified, the WG needs to have a full list of the mutual legal assistance requests.

In the first tab of the Excel file the WG should compile data from money laundering cases and typologies and organize them by jurisdiction.

Collecting data on the quantitative indicators of cross-border ML threat (Columns B–U)

In this section, the WG is to collect data on the following indicators for money laundering by jurisdiction:

- Number of money laundering convictions
- Number of money laundering prosecution
- Number of money laundering investigations
- Number of suspicious transaction reports (STRs)
- Number of FIU case files sent to law enforcement agencies (LEA)
- Total amount of seized and frozen assets
- Total amount of confiscated assets
- Originating countries of Trust and Company Service Providers (TCSP) clients (if the country has a significant TCSP sector)
- Number of Mutual Legal Assistance (MLA) requests (incoming and outgoing)
- Number of cases in which data is exchanged with foreign FIUs (incoming and outgoing)
- Total amounts associated with the MLA requests (incoming and outgoing)
- Number of Tax Information Exchange Requests (incoming and outgoing)
- Total amount of cross-border cash declarations (incoming and outgoing)
- Total number of cash smuggling cases (in borders or customs)
- Total seized or confiscated amount in cash smuggling cases (in borders or customs).

Since a large part of these indicators were used in Submodule 1.A, the same data previously collected for that part of the assessment can be re-applied here (or vice versa).

For conviction cases where multiple jurisdictions are involved, list the case for each separate jurisdiction. For example, if it was found that for a money laundering case (in which there was a guilty verdict) funds flowed from the home jurisdiction to jurisdiction X, jurisdiction Y, and jurisdiction Z, this case should be included in the numbers for all of these three countries. At the end of the analysis, the sum of cases in this column may be higher than the total number of the ML convictions in the jurisdiction.

The indicator on the country of origin of TCSP clients can be ignored if the home jurisdiction does not have a significant TSCP sector. This indicator will be more relevant for certain financial centers. The WG can complete this indicator by listing the total (estimated) number of persons by jurisdiction or use an approximate percentage (number of clients of the jurisdiction in relation to all TSCP clients). The chosen approach can be clarified in the row for “Data limitations and other issues” (row 6).

For this indicator, the WG may find the following additional (information) sources useful:

- Regulatory/Supervisory agency for TCSPs
- Registry of companies (if available)
- Surveys or interviews with TCSPs.

Collecting data on qualitative indicators of cross-border ML threat (Columns X–AB)

In this section, compile data on qualitative indicators of money laundering threats for each country.

Column X: List information obtained from dialogues with other countries

Based on information from other countries, the WG should make an assessment regarding the threat of money laundering associated with each jurisdiction. The assessment rating can rank from "low" to "high". Such information can be derived from intelligence, joint investigations, and formal/informal mutual legal assistance.

Column Y: List information obtained from interviews, or consultations with financial and other sector representatives

Based on the information from interviews, consultations or surveys by public authorities with reporting institutions make an assessment of the money laundering risk of each corridor. Choose between L (low), M (medium), or H (high).

Column Z: List information extracted from academic reports, research papers, etc.

Based on information from academic reports, or research papers from foreign public authorities, international organizations or non-profit organizations, make an assessment of the money laundering risk of each corridor. Choose L, M or H.

Column AA: List information obtained from other public sources (news, informal interviews, surveys, etc.)

Based on information regarding money laundering cases, especially cases in which no enforcement actions have been taken, from reliable news sources (domestic and international), informal interviews and surveys, make an assessment of the money laundering risk of each corridor. Choose L, M or H.

Column AB: List common ML trends, methods for particular corridors

This column lists the typologies of ML cases for the corridor with the selected jurisdiction. For input in this column, draw on the analysis of the data from Submodule 1.B (Data Collection Template) and an analysis of the data underlying the input to Columns U to X. If the analysis of these data reveals certain money laundering trends or methods for the corridors with the selected jurisdiction, record a short description of such trends and methods here. Be as specific as possible regarding the (suspected) number of cases, the value of the proceeds and the description of the typologies used.

Columns AC–AF: Summarize financial flows

In these columns, record the findings on the financial flows of the jurisdiction of tabs on financial inflows and outflows.

Columns AG–AI: Assess the money laundering threat

Based on the records of Columns B to AF, assess the money laundering threat for each jurisdiction (ranging from low to high).

Columns AJ –M: Assess the direction of the money laundering threat

By analyzing the results for Columns B to AF, assess the direction of the money laundering threat by jurisdiction. Are proceeds of crime flowing to or from other jurisdictions to be laundered?

8.3 Recording Qualitative Data on Financial Inflows and Outflows

Tabs 2 and 3 (Financial Inflows and Financial Outflows) of Submodule 1.C compile data regarding the cross-border financial flows of the home jurisdiction.

When identifying Financial Outflows (Tab 3), the same instructions as used for Financial Inflows (Tab 2) are applicable, except that they are to be considered in the reverse direction of the financial flows, starting from the country being assessed as the originator country and flowing out to other destination countries.

The aim of these sections is to place the assessment of the money laundering threat for the selected jurisdictions in a broader economic context. Here, data on the financial inflows and outflows relating to trade in goods and services, foreign direct investments, portfolio investments, and remittances are recorded and examined. By examining macroeconomic factors, deviating patterns of financial flows may be recognized (for example, financial flows might not correspond to trade flows).[3] Alternatively, the value of the flows might be much higher than normally associated with a certain trade flow. Similarly, there may be some financial flows that do not correspond to flow of goods, services or capital. Such observations may reveal the need for more vigilance on financial flows to or from certain foreign jurisdictions.

Macroeconomic indicators can mark the presence of suspicious activities. The financial stability can be affected by illicit financial flows, which may be signaled by external imbalances in the jurisdiction's Balance of Payments. For example, it has been found that jurisdictions with low AML/CFT compliance tend to have a distorted investment ratio to Gross Domestic Product (GDP), Foreign Direct Investment (FDI) ratio to GDP and financial development (ratio of credit markets to GDP).[4]

The findings on the Financial Inflows (Tab 2) and Financial Outflows (Tab 3) contribute to the overall Cross-Border Threat assessment (Tab 1) of this submodule.

Sources of information for compiling the data on financial inflows and outflows

3. From FATF (2006) on Trade-Based Money Laundering: "Trade data analysis is a useful tool to discover trade anomalies, which in turn can lead to detection, investigation and prosecution of cases of trade-based money laundering."
4. M.E. Farias, M.A. de Almeida, "Does saying 'yes' to capital inflows necessarily mean good business? The effect of anti-money laundering regulations in the Latin American and the Caribbean economies," *Economics and Politics* Vol. 26, March 2014

The main data source on a jurisdiction's overall financial inflows and outflows is the Balance of Payments. Generally, the Ministry of Finance, the Treasury, or the Central Bank will be the authority that compiles Balance of Payments data. Alternatively, it may be referred to as "Capital flows data", or "International transactions data". Securities regulators may also hold data on capital flows. A jurisdiction's Integrated Financial Management and Information System (IFMIS) might also prove a useful source of data.

The Balance of Payments is one of the key compilations for statistics on the transactions (balance of payments) and positions (international investment positions) between an economy and the rest of the world.[5] Balance of payments accounts record all monetary transactions between a country and the rest of the world. The Balance of Payments consists of different main accounts in which the transactions are recorded. These transactions include payments for:

- The export and import of goods and services
- Income flows, such as dividends and interests earned by foreigners on investments in the economy or by the economy's residents investing abroad[6]
- Financial flows, such as foreign direct investment, investment in shares, debt securities, loans, and deposits
- Financial transfers.

Balance of Payments data have been used to measure illicit financial flows.[7] However, this is not the purpose of the risk assessment. In this module, the data that are collected in the Balance of Payments are used to understand the main financial flows involving the home jurisdiction, and then triangulate that knowledge against law enforcement information on money laundering typologies for foreign jurisdictions. Determining which corridors might pose a higher money laundering threat supports the overall risk assessment exercise.

Some jurisdictions may not compile (or publish) their Balance of Payments data, or they may only maintain data for certain categories of financial flows. The availability of data needs to be verified with the Ministry of Finance, Treasury, or the Central Bank. Collect as comprehensive data as possible on financial inflows and outflows. If the jurisdiction does not maintain data on the capital accounts, data on government-related capital flows may still be available through the World Bank Global Development Finance Database.[8] This database captures inflows to multilateral, state-owned enterprises, and government-to-private-sector foreign direct investments. Data on banking flows can be requested by a jurisdiction's Central Bank from the Bank for International Settlements (BIS). The BIS publishes annual payment statistics, based on reporting by its members.

In the Balance of Payments, various categories of data are recorded. These categories are outlined below. When the jurisdiction does not compile Balance of Payment data comprehensively, or the data cannot be categorized by jurisdiction, alternative sources of these data are listed.

5. European Central Bank, "Frequently asked questions on the introduction of the Balance of Payments Manual 6", 2011 https://www.ecb.europa.eu/stats/external/bpm6/html/BPM6-faq-ECB.pdf?dad2e270978bb6eb8393bbefd94c7dc7

6 . UK Office for National Statistics, "An Introduction to the UK Balance of Payments" (accessed on March 24, 2014) www.ons.gov.uk

7 . See Victor A.B. Davies, "Capital flight and violent conflict," *World Development Report 2011* (Background note) for an overview of different methodologies for measuring estimated capital flight.

8. http://data.worldbank.org/data-catalog/global-financial-development

Jurisdictions that are financial centers should take into consideration the external banking flows between the jurisdiction and other individual financial centers on one hand, and with third countries on the other. For this purpose, consult the BIS consolidated foreign claims of reporting banks.[9]

Column A: List foreign jurisdictions

The WG should use here the list of jurisdictions compiled for assessing the money laundering threat. This list can be amended, especially in those cases when the five largest trading partners are missing from the list. If these jurisdictions are missing, add them to the list and make sure that Submodules 1.A and 1.B are completed for these jurisdictions.

Column B: Record the value of the flows for the past five years

Changes in the value of the flows may help reveal patterns that are relevant to the money-laundering context. The values of the different financial flow categories will need to be recorded for the past five years for all the selected jurisdictions.

Column C: List inflows related to trade in goods

These flows are relevant because of trade-based money laundering and fraud schemes related to over- and under-invoicing and false declarations. List the last annual value[10] of the inflows related to trade of goods with the ten largest trading partners. Insert the value per trading partner by year. Pay specific attention to jurisdictions with a trade surplus (i.e., when the export of goods is higher than imports). Also, be attentive to flows from foreign jurisdictions with which the home jurisdiction has few or no trade relations. For jurisdictions that are financial centers, the WG should note that, if their jurisdiction has a free-trade zone, trade in goods might not be recorded in a customs system.[11] Alternative data sources for trade in goods are the following:

- UN COMTRADE (joint database of World Bank, UN, and OECD on bilateral trade flows)[12]
- UN International Merchandise Trade Statistics
- UNCTAD TRAINS (Trade Analysis and Information System)[13]
- World Bank/UN World Integrated Trade Solution (WITS) (World Trade Atlas).[14]

Column D: list inflows related to trade in services

For this variable, insert the annual value of the inflows related to trade in services for the selected jurisdictions. Insert the value per trading partner. Official trade data will include data on the import and export of inter alia financial services,[15] insurance and pension services, telecommunications, computer

9 http://www.bis.org/statistics/consstats.htm

10. BOP code: 100, (Current account/Goods),(2 sub levels) IMF, Balance of Payments Coding System (topical list of codes). See: http://www.imf.org/external/np/sta/bopcode/topical.htm

11. See *IMF BOP Manual*, p. 153, para. 10.18

12. http://comtrade.un.org/

13. This is the most comprehensive database at the most disaggregated level of custom coding of products (Harmonized System). Includes information on import flows by origin from more than 150 countries.

14. WITS is a software application that integrates trade databases, including UNCTAD-TRAINS, WTO, IDB and CTS databases and UN COMTRADE. *Manual on Statistics of International Trade in Services* (2002).

15. Financial services include financial intermediary and auxiliary services, such as (cross-border) deposit taking and lending, letters of credit, credit card services, commissions and charges related to financial leasing, clearing of payments etc. Also included are financial advisory services, custody of financial assets, financial asset management, monitoring services, liquidity

and information services and other business services.[16] Data on the export of trade in services can be relevant if it is suspected that non-residents seek the help of the home jurisdiction's business service providers to launder money, especially if the trade in services relating to the main economic activities in the home jurisdiction is low. Data on the import of trade in services might indicate that domestic residents seek foreign service providers to launder money.[17]

Column E: List Foreign Direct Investment (FDI)

These flows are relevant for the money-laundering context, since much of FDI can be relatively liquid (acquisition of shares in companies by non-residents and the purchase of real estate by non-residents, etc.). The county may decide to further breakdown the FDI column in order to better see the real estate investments, share acquisitions, or any other specific item. FDI is recorded in the financial account of the Balance of Payments. Alternative sources for data on FDI are the following:

- International Transactions Reporting System (ITRS) records a large amount of information on transactions from banking records. Note that the ITRS only records cash transactions and might not always capture FDI transactions in the domestic currency.[18]
- The Treasury Check Information System (TICS) database[19] lists the country of origin of investments. It covers investments related to both the government (short-term securities, long-term securities, and in-company bonds) and the private sector (equity, corporate bonds, and derivatives).

Column F: List portfolio investments[20]

Portfolio investment is considered to be a common channel for illicit flows.[21] Portfolio investment includes cross-border transactions and positions involving debt or equity securities, other than those included in direct investment or reserve assets. It covers securities traded on financial markets. Data on Portfolio Investment can be found in the financial account in the Balance of Payments.[22] Financial assets under portfolio investment include debt securities[23]; listed shares;[24] unlisted shares;[25] money market fund shares/units; [26]and other investment fund shares/units.[27] The largely anonymous relationship between issuers and holders and the degree of trading liquidity in the instruments could make this type of investment more prone to money laundering. The trade in financial assets is, of course, often a legitimate business activity. Furthermore, a large part of the investments is likely made through stockbrokers in large

providing services, risk assumption services, merger and acquisition services, stock exchange services and trust services. See *IMF BOP Manual*, p. 172 para. 10.118.

16. Other business services include, *inter alia*: research and development services; professional and management consulting services, which include legal services, accounting, management consulting, and managerial services; and operating leasing.

17. BOP Code: Services 200, Financial Services: 260, Royalties and license fees 266, Other business services 268

18. *IMF BoP Compilers' Guide* (2013) on ITRS: "In some central banks, the ITRS evolved as data-reporting system that was previously built on an exchange control system; as economies dismantled exchange control, the ITRS became a less comprehensive source for balance of payments statistics."

19. http://www.fms.treas.gov/tcis/index.html

20. BOP code 339

21. Farias, de Almeida (2014)

22. Portfolio investment becomes FDI when a direct investor owns equity that entitles it to > 10% of the voting power in the direct investment enterprise: see *IMF BOP Manual* p. 101, para. 6.12 and *OECD Benchmark Definition of Foreign Direct Investments* (2008)

23. AF3 Debt securities (2008 SNA Financial Assets and Liabilities Classification)

24. AF5 11 Listed shares (2008 SNA Financial Assets and Liabilities Classification)

25. AF5 12 Unlisted shares (2008 SNA Financial Assets and Liabilities Classification)

26. AF5 21 Money market fund shares/units (2008 SNA Financial Assets and Liabilities Classification)

27. AF 22 other investment fund shares/units (2008 SNA Financial Assets and Liabilities Classification)

financial centers, which may distort the data and complicate the identification of beneficial owners and their jurisdiction of origin.

An additional source of data on Portfolio investments is SWIFT data. Permission to access SWIFT data must be given by individual financial and reporting institutions. Aggregate data may possibly be purchased from SWIFT by the Central Bank. Further information can be obtained from SWIFT on request).

Column G: List remittances

Remittances are cash and noncash items that flow through formal banking channels, such as via electronic wire, or through informal channels, such as money or goods carried across borders, often by migrant workers.[28] Remittances transferred through informal channels might not always be recorded by the Remittances data in the Balance of Payments. An alternative source for Remittances data is the Annual Remittances Data and Bilateral Remittance Matrix by the World Bank.[29]

Column H: Total

Add the sum of the values in Columns C–G and list the total value of these annual flows in this column per jurisdiction.

Columns I–L: Determine the economic rationale for the financial flows figures

The WG is expected to consider the values of the annual financial flows to and from the selected jurisdictions, and make an assessment of whether the recorded values correspond with the real economic relationships with foreign jurisdictions. If the figures correspond (partially) with the economic reality, indicate that the rationale for the figures is "Clear" or "Partially clear". If the WG finds that the figures do not reflect the real economic relationship with a foreign jurisdiction, the WG should indicate that the rationale is "Unclear."

8.4 Assessing the Money Laundering Threat for each Corridor

As explained earlier, the module on Cross-border threat does not include any built-in formulas or calculations. Consider all the indicators for a particular country, and then make a judgment about the current level, direction, and trend of the money laundering threat (incoming or outgoing) in each corridor.

Assess the level of cross-border money laundering threat for each corridor by taking into account the inputs on the:

- Quantitative indicators of money laundering threats (Tab 1)
- Qualitative indicators of money laundering threats (Tab 1)
- Quantitative indicators of overall financial flows (Tab 3, summarized in Tab 1).

It is expected that the money laundering threat for the jurisdictions is assessed relative to each other. Take into consideration the home jurisdiction's GDP and estimated domestic proceeds of crimes.

9. ASSESSING THE FUTURE TRENDS

28. IMF BOP Manual, Appendix 5 Remittances, p. 272 ff.
29. Based on household surveys
http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTDECPROSPECTS/0,,contentMDK:22759429~pagePK:64165401~piPK:64165026~theSitePK:476883,00.html

For a comprehensive understanding of the risks, it is essential to also apprehend the possible threats and risks that may arise from future developments. To support a forward-looking perspective, each tab in Module 1.A includes columns to assess future trends of the identified threats.

Beyond the trend analysis already included in the tool, the threat assessment team should also conduct an assessment of any other potentialthreats that might not have been included in the assessment, because the threat has not yet materialized, or currently considered to be insignificant or because there is insufficient data and information.

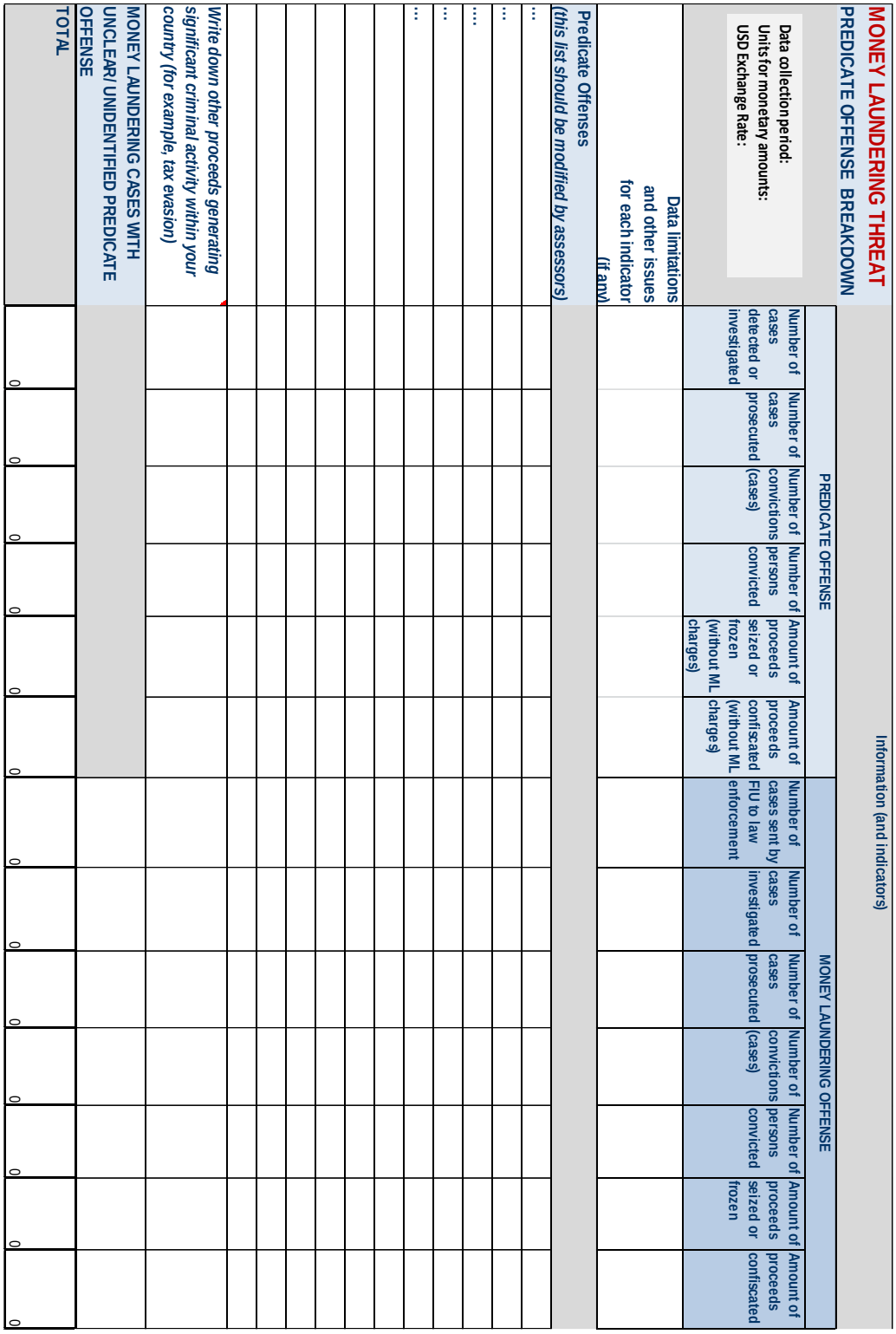
In collaboration with all other teams, the threat assessment team should also assess how the identified threats may change in the short and medium term and identify other threats that may emerge as a result of possible changes in:

- The crime environment
- Sectors
- Products, services, or channels
- Bilateral/multilateral corridors
- Geographic, politic, social, and/or economic factors.

The country's national risk assessment report should also include a discussion of the future trends and emerging threats.

ANNEX - SCREENSHOTS OF EXCEL MODULES

MODULE 1.A - ML THREAT ASSESSMENT (Predicate Offense Breakdown Tab)



MONEY LAUNDERING THREAT

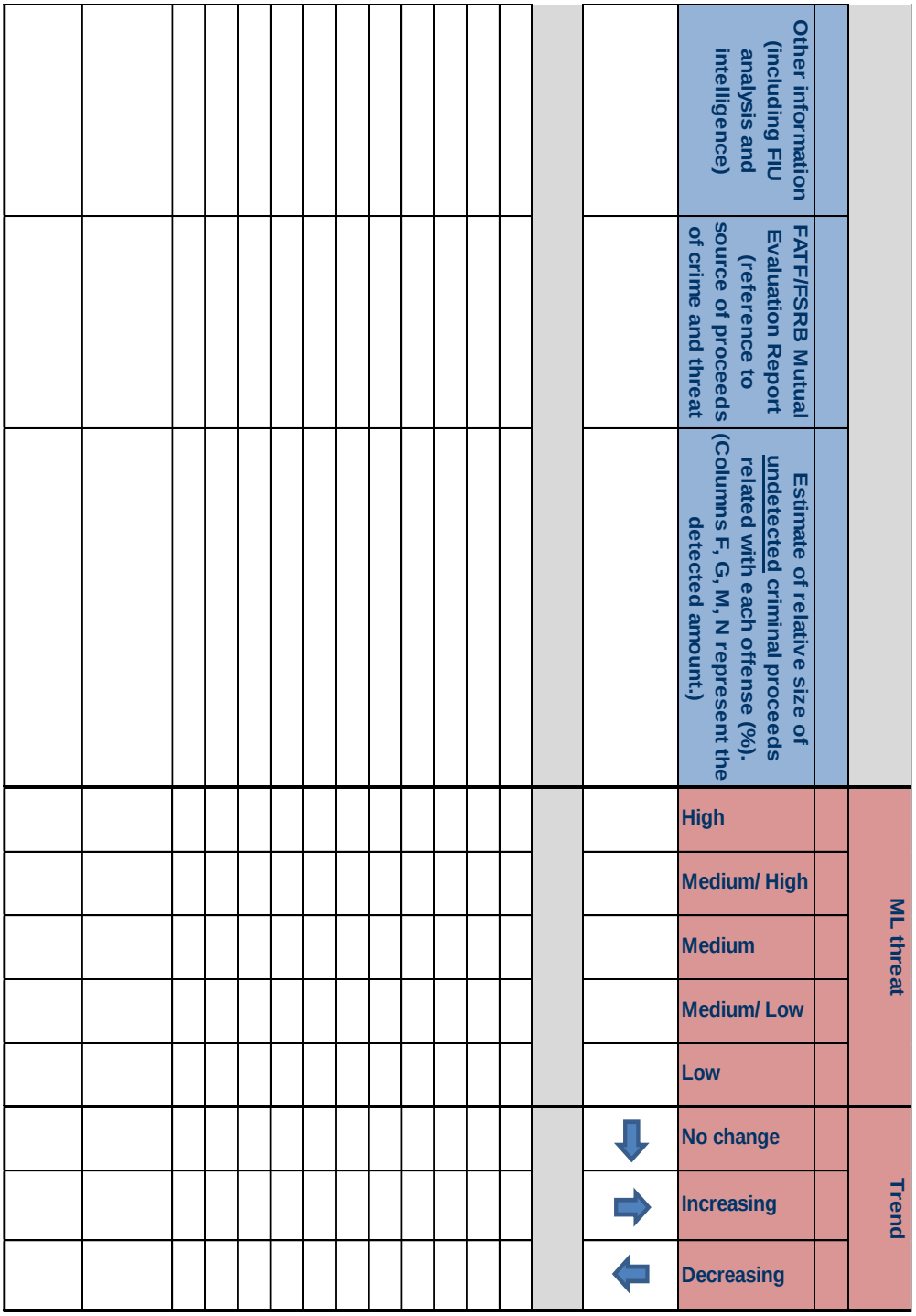
PREDICATE OFFENSE BREAKDOWN

Data collection period:
Units for monetary amounts:
USD Exchange Rate:

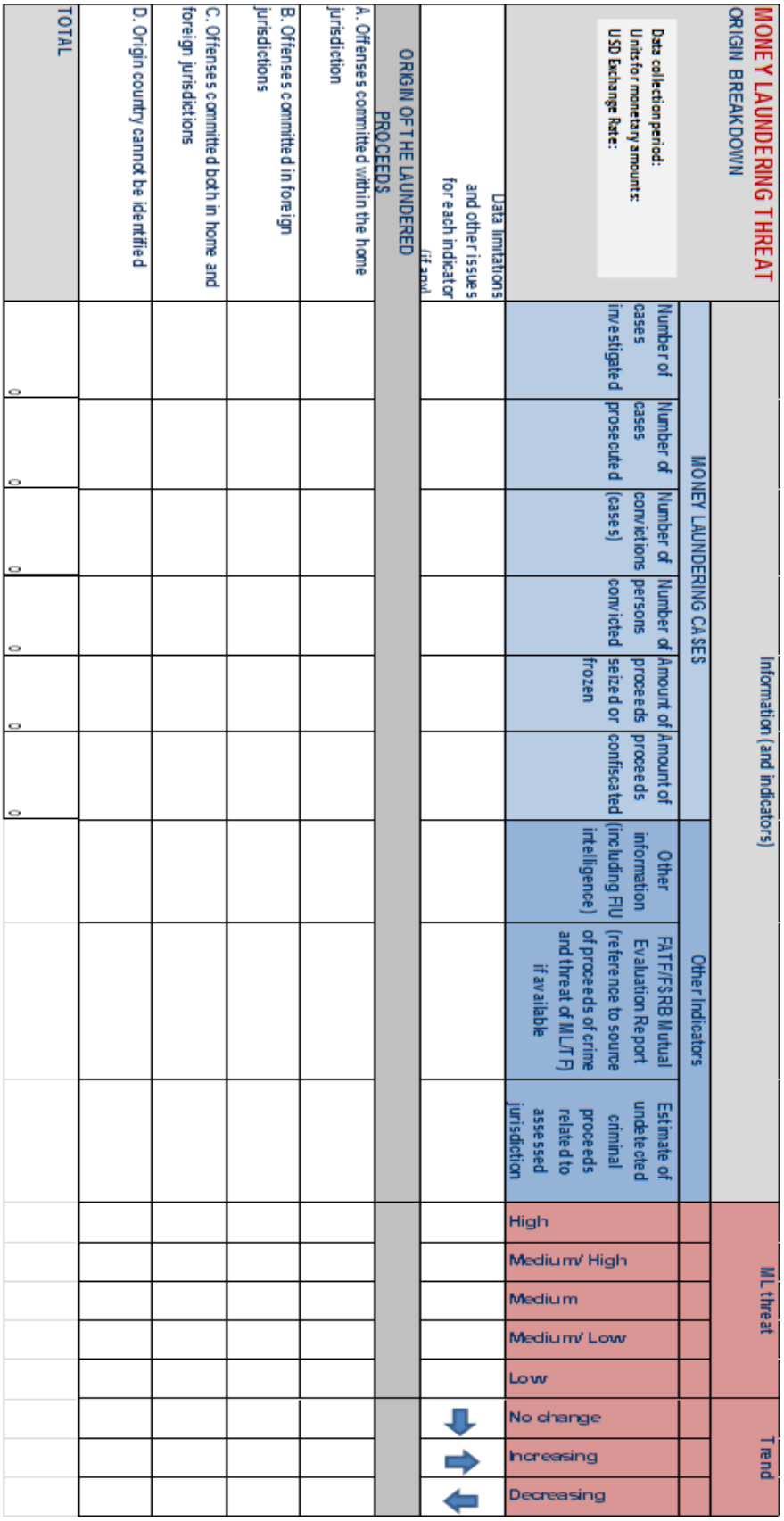
Information (and indicators)

Predicate Offenses (this list should be modified by assessors)	Data limitations and other issues for each indicator (if any)	PREDICATE OFFENSE						MONEY LAUNDERING OFFENSE						
		Number of cases detected or investigated	Number of cases prosecuted	Number of convictions (cases)	Number of persons convicted	Amount of proceeds seized or frozen (without ML charges)	Amount of proceeds confiscated (without ML charges)	Number of cases sent by FIU to law enforcement	Number of cases investigated	Number of cases prosecuted	Number of convictions (cases)	Number of persons convicted	Amount of proceeds seized or frozen	Amount of proceeds confiscated
…														
…														
….														
…														
…														
Write down other proceeds generating significant criminal activity within your country (for example, tax evasion)														
MONEY LAUNDERING CASES WITH UNCLEAR/ UNIDENTIFIED PREDICATE OFFENSE														
TOTAL		0	0	0	0	0	0	0	0	0	0	0	0	0

MODULE 1.A - ML THREAT ASSESSMENT (Predicate Offense Breakdown Tab)



MODULE 1.A - ML THREAT ASSESSMENT (Origin Breakdown Tab)



MONEY LAUNDERING THREAT

ORIGIN BREAKDOWN

Data collection period:
Units for monetary amounts:
USD Exchange Rate:

Information (and indicators)

MONEY LAUNDERING CASES

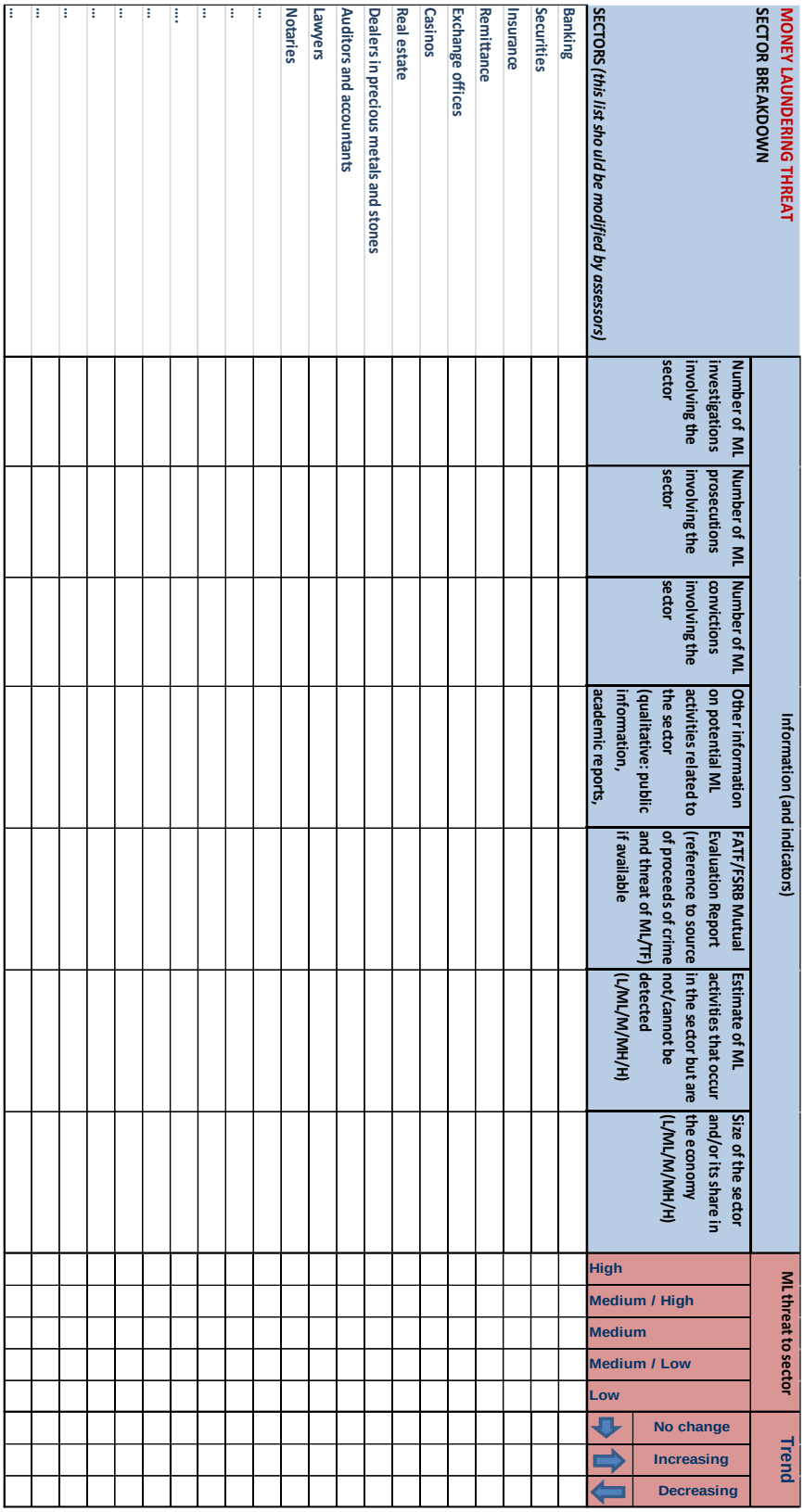
Other Indicators

ML threat

Trend

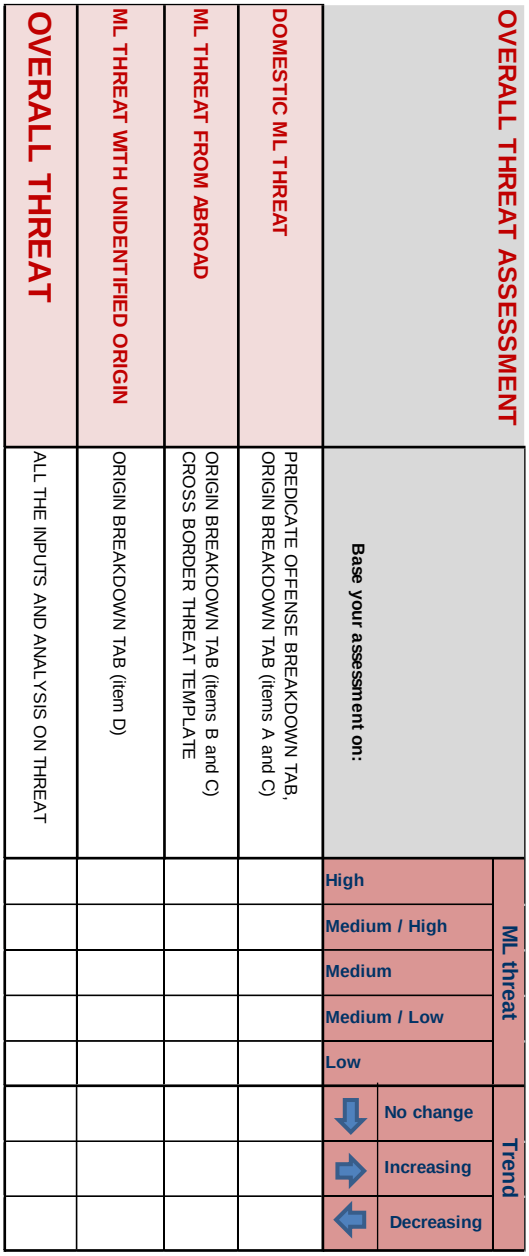
ORIGIN OF THE LAUNDERED PROCEEDS	Data limitations and other issues for each indicator (if any)	Number of cases investigated	Number of cases prosecuted	Number of convictions (cases)	Number of persons convicted	Amount of proceeds seized or frozen	Amount of proceeds confiscated	Other information (including FIU intelligence)	FATF/FSRB Mutual Evaluation Report (reference to source of proceeds of crime and threat of ML/TF) if available	Estimate of undetected criminal proceeds related to assessed jurisdiction			TOTAL
A. Offenses committed within the home jurisdiction											High		
B. Offenses committed in foreign jurisdictions											Medium/ High		
C. Offenses committed both in home and foreign jurisdictions											Medium		
D. Origin country cannot be identified											Medium/ Low		
TOTAL		0	0	0	0	0	0				Low		
											No change		
											Increasing		
											Decreasing		

MODULE 1.A - ML THREAT ASSESSMENT (Sector Breakdown Tab)



MONEY LAUNDERING THREAT SECTOR BREAKDOWN	Information (and indicators)								ML threat to sector		Trend
SECTORS (*this list sho uld be modified by assessors*)	Number of ML investigations involving the sector	Number of ML prosecutions involving the sector	Number of ML convictions involving the sector	Other information on potential ML activities related to the sector (qualitative: public information, academic reports,	FATF/FSRB Mutual Evaluation Report (reference to source of proceeds of crime and threat of ML/TF) if available	Estimate of ML activities that occur in the sector but are not/cannot be detected (L/ML/M/MH/H)	Size of the sector and/or its share in the economy (L/ML/M/MH/H)	High		
Banking								Medium / High		
Securities								Medium		
Insurance								Medium / Low		
Remittance								Low		
Exchange offices									No change	
Casinos									Increasing	
Real estate									Decreasing	
Dealers in precious metals and stones										
Auditors and accountants										
Lawyers										
Notaries										
…										
…										
….										
…										
…										
…										
…										
…										

MODULE 1.A - ML THREAT ASSESSMENT (Overall Assessment Tab)



OVERALL THREAT ASSESSMENT	Base your assessment on:	ML threat	Trend
DOMESTIC ML THREAT	PREDICATE OFFENSE BREAKDOWN TAB, ORIGIN BREAKDOWN TAB (items A and C)	High	No change
ML THREAT FROM ABROAD	ORIGIN BREAKDOWN TAB (items B and C) CROSS BORDER THREAT TEMPLATE	Medium / High	Increasing
ML THREAT WITH UNIDENTIFIED ORIGIN	ORIGIN BREAKDOWN TAB (item D)	Medium	Decreasing
OVERALL THREAT	ALL THE INPUTS AND ANALYSIS ON THREAT	Medium / Low	
		Low	

MONEY LAUNDERING THREAT **CASE BASED DATA COLLECTION TEMPLATE**	**CONVICTED ML CASES**				**PROSECUTED ML CASES**				**INVESTIGATED ML CASES**			
Case name or number	**EXAMPLE (case ref. 12345)**	**…**	**…**	**…**	**…**	**…**	**…**	**…**	**…**	**…**	…	…
Sectors involved	Banking, remittance, real estate, and legal											
Number of entities involved (with sector breakdowns)	2 banks, 1 remittance company, 1 lawyer											
Name of the institutions involved (can be kept confidential)	Bank A, bank B											
Number of bank accounts involved	5											
Average amount in detected bank accounts	50,000 USD											
Number of money transfers	10											
Average amount in money transfers	2000 - 3000 USD											
Financial products/services involved	Money transfer services, bank accounts, and checks											
Predicate offense	Drug trafficking											
Total detected amount	….. USD (or local currency)											
Total seized amount	….. USD (or local currency)											
Total confiscated amount	….. USD (or local currency)											
Number of citizens involved	12											
Number of non-citizens involved	2											
Destination countries (where the money goes)	Country A, country B											
Originator countries (where the money comes from)	Domestic											
Regions involved	Region A, region B, etc.											
Summary of the techniques and methods used in ML	Use of structuring and real estate sector											
Trigger for the investigation	STR to FIU											
Result of the investigation	Prosecution, conviction											
Other important points	….											
Short narrative of the case	….											

MODULE 1.C - CROSS-BORDER THREAT ASSESSMENT

						Qualitative indicators of ML threat (linked to each country)	Information obtained from dialogues with other countries (L/M/H)
							Information obtained from interviews, and consultations with financial and other sector representatives (L/M/H)
							Information extracted from academic reports, research papers etc. (L/M/H)
							Information obtained from public sources (news, informal interviews, surveys, etc.) (L/M/H)
							Common ML trends/methods for the corridor (description)
						Financial flows (summary)	Financial inflows (Output of financial inflows tab)
							Rationale explaining inflows
							Financial outflows (Output of financial outflows tab)
							Rationale explaining outflows
						ML THREAT	High
							Medium/ High
							Medium
							Medium/ Low
							Low
						DIRECTION OF THE THREAT	Incoming
							Outgoing
							Both Directions
							Unclear
						TREND	No change
							Increasing
							Decreasing

							Data collection period: Units for monetary amounts: USD Exchange Rate :	
					JURISDICTION/COUNTRY	Explanations on data limitations and other issues.		Quantitative indicators of ML threat (linked to each country)
				Country A			Number of ML convictions	
							Number of ML prosecutions	
							Number of ML investigations	
							Number of STRs received by FIU	
							Number of FIU case files sent to LEA	
							Total amount of frozen/seized assets	
							Total amount of confiscated assets	
							Origin of countries of TCSP clients (%)	
							Number of mutual legal assistance (MLA) requests (Incoming)	
							Number of cases in which data is exchanged with foreign FIUs (Incoming)	
							Other forms of International Assistance (Incoming)	
							Total amounts associated with MLA requests (Incoming)	
							Number of tax information exchange requests (Incoming)	
							Total amount of cash declarations (Incoming)	
							Undeclared cash (seized/confiscated) (Incoming)	
							Number of mutual legal assistance (MLA) requests (Outgoing)	
							Number of cases in which data is exchanged with foreign FIUs (Outgoing)	
							Other forms of International Assistance (Outgoing)	
							Total amounts associated with MLA requests (Outgoing)	
							Number of tax information exchange requests (Outgoing)	
							Total amount of cash declarations (Outgoing)	
							Undeclared cash (seized/confiscated) (Outgoing)	
				Country B				
				Country C				
				...				
				...				

MODULE 1.C - CROSS-BORDER THREAT ASSESSMENT (Financial Inflows Tab)

Financial inflows (million USD)		Financial inflows (Annual figures)						RATIONALE			
JURISDICTION/COUNTRY	Year	Inflows related to trade in goods	Inflows related to services	Foreign Direct Investment (FDI)	Portfolio investments	Remittances	TOTAL	Unclear	Clear	Partially clear	If clear, or partially clear, please give a brief explanation
Country A											
	2013										
	2012										
	2011										
	2010										
	2009										
Country B											
	2013										
	2012										
	2011										
	2010										
	2009										
Country C											
	2013										
	2012										
	2011										
	2010										
	2009										
....	2013										
	2012										
	2011										
	2010										
	2009										
...											

MODULE 1.C. - CROSS-BORDER THREAT ASSESSMENT (Financial Outflows Tab)

Financial outflows (million USD)								RATIONALE			
JURISDICTION/COUNTRY	Year	Outflows related to trade in goods	Outflows related to services	Foreign Direct Investments (FDI)	Portfolio investments	Remittances	TOTAL	Unclear	Clear	Partially clear	If clear, or partially clear, please give a brief explanation
Country A											
	2013										
	2012										
	2011										
	2010										
	2009										
Country B											
	2013										
	2012										
	2011										
	2010										
	2009										
Country C											
	2013										
	2012										
	2011										
	2010										
	2009										
...											
	2013										
	2012										
	2011										
	2010										
	2009										
...											