



FATF GUIDANCE

# Money Laundering National Risk Assessment Guidance

November 2024





The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit [www.fatf-gafi.org](http://www.fatf-gafi.org)

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2024), Money Laundering National Risk Assessment Guidance, FATF, Paris,  
<https://www.fatf-gafi.org/en/publications/Methodsand trends/Money-Laundering-National-Risk-Assessment-Guidance.html>

© 2024 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: [contact@fatf-gafi.org](mailto:contact@fatf-gafi.org))

Photocredits coverphoto © Shutterstock/SuPatMaN

# Table of Contents

- Acronyms..... 3**
- Executive Summary ..... 5**
- Introduction ..... 6**
  - Purpose, Scope and Objectives ..... 6
  - Core FATF Obligations Related to ML NRAs ..... 8
  - Structure ..... 8
  - Methodology ..... 9
  - Key Concepts Relevant to Assessing and Understanding ML Risks ..... 9
- Section 1: NRA Preparation and Set-up..... 11**
  - Political Commitment to Conduct the NRA ..... 11
  - An Inclusive National Mechanism to Assess Risk..... 12
  - Scoping and Objective Setting..... 17
  - Collection of Information and Data..... 20
  - Section Conclusion ..... 30
- Section 2: Assessing and Understanding ML Risks ..... 32**
  - Environmental Scan..... 32
  - Analytical Process..... 34
  - Analysis of Threats..... 35
  - Analysis of Vulnerabilities ..... 40
  - Risk Assessment..... 43
  - Horizon Scanning..... 45
  - Section Conclusion ..... 47
- Section 3: Post-NRA Actions ..... 48**
  - Align AML Strategies and Policies with Risk ..... 48
  - Outreach and Stakeholder Engagement ..... 59
  - Feedback and Improving the NRA Process ..... 61
  - Section Conclusion ..... 64
- Annex A. Types of Risk Assessments that Complement the NRA..... 65**
  - Sectoral and Thematic Risk Assessments..... 65
  - Supranational and Subnational Risk Assessments ..... 66
- Annex B. High-level Summary of Responses to Public Consultation..... 71**

## Acronyms

<b>AI</b>	Artificial Intelligence
<b>AML</b>	Anti-Money Laundering
<b>ASEAN</b>	Association of Southeast Asian Nations
<b>CDD</b>	Customer Due Diligence
<b>CFATF</b>	Caribbean Financial Action Task Force
<b>CFT</b>	Counter Financing of Terrorism
<b>CFTP</b>	Countering the Financing of Terrorism and Proliferation
<b>DNFBP</b>	Designated Non-Financial Business and Professions
<b>EAG</b>	Eurasian Group
<b>EDD</b>	Enhanced Due Diligence
<b>EU</b>	European Union
<b>FATF</b>	Financial Action Task Force
<b>FI</b>	Financial Institution
<b>FIU</b>	Financial Intelligence Unit
<b>FSC</b>	Financial Security Committee
<b>FSRB</b>	FATF-Style Regional Body
<b>ICRG</b>	International Co-operation Review Group
<b>IDB</b>	Inter-American Development Bank
<b>IFI</b>	International Financial Institution
<b>IMF</b>	International Monetary Fund
<b>INR</b>	Interpretive Note to Recommendation
<b>IO</b>	Immediate Outcome
<b>IOSCO</b>	International Organization of Securities Commissions
<b>KPI</b>	Key Performance Indicator
<b>KYC</b>	Know Your Customer
<b>LEA</b>	Law Enforcement Agency

#### 4 | Money Laundering National Risk Assessment Guidance

---

<b>MER</b>	Mutual Evaluation Report
<b>ML</b>	Money Laundering
<b>MLA</b>	Mutual Legal Assistance
<b>MOU</b>	Memorandum of Understanding
<b>NPO</b>	Non-Profit Organisation
<b>NRA</b>	National Risk Assessment
<b>PESTEL</b>	Political, Economic, Social, Technological, Environmental, and Legal
<b>PF</b>	Proliferation Financing
<b>PPP</b>	Public-Private Partnership
<b>R</b>	Recommendation
<b>RBA</b>	Risk-Based Approach
<b>SAR</b>	Suspicious Activity Report
<b>SDD</b>	Simplified Due Diligence
<b>SNRA</b>	Supranational Risk Assessment
<b>SRB</b>	Self-Regulatory Bodies
<b>STR</b>	Suspicious Transaction Report
<b>TBML</b>	Trade-based money laundering
<b>TF</b>	Terrorist Financing
<b>UNODC</b>	United Nations Office on Drugs and Crime
<b>VA</b>	Virtual Asset
<b>VASP</b>	Virtual Asset Service Provider
<b>WBG</b>	World Bank Group

---

## 1. Executive Summary

Money laundering risk understanding is a foundational element on which a national AML/CFT system is built. This is reinforced by Recommendation 1 of the FATF Standards, which requires countries to “identify, assess and understand” its money laundering risks, and to take action to ensure that these risks “are mitigated effectively”.

The development of an accurate and up-to-date risk understanding is an ongoing, dynamic process for a country. A process that necessitates responding to changing environmental factors, constantly assessing new information and scanning the horizon for risks that may be emerging or materialising. Accordingly, it is important that a country takes a structured and coherent approach to developing an up-to-date risk understanding. Once such common approach for a country to take is through the conduct of a National Risk Assessment (NRA).

An NRA is a comprehensive process used by countries to identify, assess, and understand the ML and/or TF risks they face. This process involves evaluating threats and vulnerabilities, determining the level of risk, and developing strategies aligned to ML risks. This includes taking enhanced measures where risks are higher and taking simplified or lesser measures where risks are lower. While the end result of the process may or may not be a written product, the understandings reached, and follow-on actions taken are of paramount importance.

The NRA provides an evidence-based foundation for informed policymaking, resource allocation, and the implementation of effective AML/CFT measures. It ensures that national strategies are aligned with the specific risk landscape of the country and that they address both domestic and international threats to the extent they are connected to the country.

The purpose of this document is to assist countries in conducting an NRA focused on the assessment of money laundering risks. This document has been developed considering the experience of a range of countries from across the FATF Global Network in the last decade – more than 90 contributed to this guidance – and is meant to demonstrate good practices that have been used by countries to assist others in tailoring these good practices into their own national context. This document contains three sections:

- i. **Section 1: NRA Preparation and Set-up** – This section identifies the prerequisites to a successful NRA. It covers such key foundational parts of the NRA such as political commitment, an inclusive NRA mechanism, objective setting, and the acquisition of information and data. These steps are not necessarily linear steps, but all should be considered and in place before the analytical work of the NRA can begin.
- ii. **Section 2: Assessing and Understanding Money Laundering Risks** – This section provides a linear, structured approach for countries to follow in conducting their analysis of threats, vulnerabilities, and risks. There is no set methodology that countries must follow, and a country’s NRA process should have regard to its capacity, as well as its unique risk and context. However, the series of steps outlined here has been identified as a good practice
- iii. **Section 3: Post-NRA Actions** – This section identifies simultaneous practices that a country should undertake after the conclusion of the analytical process. It covers the measures that a country could take to ensure that its ML mitigation measures are commensurate with the risks identified, the communication of the NRA’s findings, and refining of the NRA process.

## Introduction

### Purpose, Scope and Objectives

Identifying, assessing and understanding money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks is an essential part of the implementation of a national anti-money laundering/countering the financing of terrorism (AML/CFT) regime which includes laws, regulations, enforcement and other measures to mitigate ML/TF risks. The results of a national risk assessment (NRA) should provide useful information to financial institutions (FIs) designated non-financial businesses and professions (DNFBPs) and virtual asset service providers (VASPs) to support their own assessments and risk mitigation measures. Properly understanding ML/TF risks informs and supports countries' application of AML/CFT measures that are proportionate with the risks, i.e. the risk-based approach (RBA) that is central to the FATF Standards and should assist countries in prioritisation and efficient allocation of resources.

The FATF has underlined this importance by introducing Recommendation 1 in 2012, which emphasises the need to identify, assess, understand and mitigate ML/TF risks as a fundamental basis for the effective implementation of the FATF's 40 Recommendations. In line with the revised Standards many countries have conducted NRAs to consolidate and align their ML/TF risk understanding at a national level. This has also become a key step for many countries in demonstrating their understanding of risks and improving their ability to combat ML/TF.

To assist countries in these efforts, the FATF produced guidance for conducting national ML and TF risk assessments in 2013.<sup>1</sup> Since then, countries across the FATF Global Network have gained substantial experience in developing NRAs, leading to the refinement of guidance and methodologies. The FATF, recognising the evolution in risk assessments, updated its TF NRA guidance in 2019<sup>2</sup> and following changes to the FATF Standards, introduced guidance on PF NRAs in 2021.<sup>3</sup> This present guidance document updates the 2013 guidance, but addresses only ML NRAs.

An ML NRA is a comprehensive evaluation conducted by a country to identify and assess its ML risks. It involves analysing the threats and vulnerabilities of ML across a number of factors, including sectors, activities, geographic locations, client types, products and channels and developing evidence-based risk mitigation measures to strengthen the country's AML system. An ML NRA promotes a holistic approach to risk and aims to develop a baseline understanding of risk among all stakeholders involved the AML system. An NRA should encompass cross-border risks, and its impact could extend beyond the country's borders, supporting the understanding and reduction of ML in a national context, as well as an international one.

Despite marked progress in this area in the last decade, challenges persist. The FATF's Report on the State of Effectiveness and Compliance with the FATF Standards<sup>4</sup> published in April 2022

---

<sup>1</sup> FATF (2013), National Money Laundering and Terrorist Financing Risk Assessment Guidance, [National money laundering and terrorist financing risk assessment \(fatf-gafi.org\)](https://www.fatf-gafi.org/publications/nmlr/Pages/default.aspx)

<sup>2</sup> FATF (2019), Terrorist Financing Risk Assessment Guidance, [Terrorist Financing Risk Assessment Guidance \(fatf-gafi.org\)](https://www.fatf-gafi.org/publications/tf/Pages/default.aspx)

<sup>3</sup> FATF (2021), Proliferation Financing Risk Assessment Guidance, [www.fatf-gafi.org/content/fatf-gafi/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html](https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html)

<sup>4</sup> FATF (2022), Report on the State of Effectiveness and Compliance with the FATF Standards, [www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Effectiveness-compliance-standards.html](https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Effectiveness-compliance-standards.html)

showed that although compliance with R.1 increased by 24% through the 4th round follow-up process, improvements are needed particularly in data collection, stakeholder training and awareness, and effective communication of the NRA findings. The collective experience and knowledge gained from the Global Network should be leveraged, as well as the views of technical assistance providers and academics researching this topic, to promote sustainable and effective action to improve AML systems worldwide. This guidance takes forward the basic principles explored in the FATF's 2013 ML/TF NRA guidance and provides practical examples and best practices from the Global Network reflecting the decade of experience countries have developing NRAs.

This guidance draws from various sources, including inputs received from 90 countries across the FATF Global Network in two questionnaires, Mutual Evaluation Reports (MERs), published NRAs, studies from international bodies, like the World Bank Group (WBG) and the International Monetary Fund (IMF) and the results of a public consultation. It aims to provide countries with guidance and best practices on conducting ML NRA. It emphasises the importance of understanding the evolving ML risk landscape, addresses common challenges and identifies good practices in conducting NRAs with a focus on procedural and structural aspects essential for impactful risk assessments, based on the experience of countries from across the Global Network. This guidance provides a foundational concept and globally recognised principles to guide countries in their decision-making process, offering a flexible framework to facilitate a comprehensive evaluation of ML risks at a national level.

Ultimately, the objective of this guidance is to provide countries with practical advice that will enhance the effectiveness of ML NRA, driving informed decision making and resource allocation to take an RBA to preventing and mitigating the identified ML risks.

This guidance document is not a FATF Standard and is therefore not intended to designate specific actions necessary to meet obligations under Recommendation 1 and INR 1 or any other FATF Standards. Criteria for technical compliance and for assessing may be found in the FATF assessment methodology. The practices described in this guidance are intended to serve as examples that may facilitate implementation of obligations in a manner compatible with the FATF Standards.

This guidance has been drafted with the goal of catering to the diverse needs of countries, recognising those needs will vary depending on the maturity level of the risk assessment mechanism of each country. Consequently, the guidance aims to provide the key concepts and activities that countries have sought guidance on, with adequate support and practical tools that can respond to country needs depending on whether the country is in the initial stages of preparing its first NRA, or it already has a well-established and effective mechanism in place. The guidance aims to promote that all countries, can effectively identify, assess and understand their risks, recognising that the level of detail and complexity will vary based on a country's risk and context. The guidance is designed to offer flexibility, ensuring relevance and applicability across the Global Network.

The guidance includes selected good practices from a wide variety of countries across the FATF Global Network. Countries with less mature NRA processes often face challenges in developing their NRA. Many of these countries are in the earlier stages of establishing a culture of ongoing risk assessment and may encounter obstacles such as limited resources, insufficient data and lack of experienced personnel. Recognising these difficulties, the guidance outlines key strategies to ensure the NRA is effective, providing tailored recommendations to address specific challenges



faced. The diversity of good practices showcases how countries with different risks and context, legal systems, and maturity of AML measures have had success in implementing aspects of the Recommendation 1.

### Core FATF Obligations<sup>5</sup> Related to ML NRAs

This section outlines the FATF's requirements for identifying and assessing ML risk at the country level. A key component of the FATF Standards is understanding ML risks and the RBA, which requires countries to tailor their AML measures according to identified risks. The following FATF Recommendations are core to ML NRAs:

- **Recommendation 1 (R.1):** R.1 identifies that “Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively”.
- **Interpretative Note to Recommendation 1 (INR.1):** INR.1 clarifies that countries should take steps to identify and assess their ML risks on an “ongoing basis” to: (1) inform potential changes to the country's AML regime, including changes to laws, regulation; and (2) assist in the allocation and prioritisation of AML resources by competent authorities. Countries should have a mechanism to provide information on the results of the risk assessment(s) to all relevant competent authorities and self-regulatory bodies (SRBs), FIs, and DNFBPs
- **Recommendation 2 (R.2):** R.2 identifies that, “Countries should have national AML/CFT/CPF policies, informed by the risks<sup>1</sup> identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.”

### Structure

This guidance is structured in three sections:

**Section 1: NRA Preparation and Set-up** – This section identifies the prerequisites to a successful NRA. It covers such key foundational parts of the NRA such as political commitment, an inclusive NRA mechanism, objective setting and the acquisition of information and data. These steps are not necessarily linear steps, but all should be considered and in place before the analytical work of the NRA can begin.

**Section 2: Assessing Money Laundering Risks** – This section provides a linear, structured approach for countries to follow in conducting their analysis of threats, vulnerabilities and risks. There is no set methodology that countries must follow, and a country's NRA process should have regard to its capacity, risk and context, but this series of steps has been identified as a good practice.

---

<sup>5</sup> There are numerous other parts of the FATF Standards that involve the risk-based approach, such as R.15/INR.15, R.10, R.24/25 and INR.24/25, R.26 and R.28. This section refers to parts considered to be core to ML NRAs.

**Section 3: Post-NRA Actions** – This section identifies parallel practices that a country should undertake after the conclusion of the analytical process. It covers the measures that a country could take to ensure that its ML mitigation measures are commensurate with the risks identified., the communication of the NRA’s findings and refining of the NRA process.

## Methodology

This update to FATF’s ML guidance was co-led by Mexico and Hong Kong, China, with input from a project team of 33 FATF and FATF-Style Regional Bodies (FSRB) members, and observer organisations.<sup>6</sup>

This guidance incorporates input from a number of delegations within the FATF Global Network on their experiences, challenges and good practices in assessing ML risk. 59 delegations provided responses to the first questionnaire and 70 delegations to the second follow-up questionnaire, which sought input particularly on the main challenges and lessons learned in all of the key areas outlined above. The FATF Secretariat also conducted a review of NRAs from 69 FATF and FSRB members and MERs from across the Global Network.

The project team sought input from the private sector through the FATF’s Private Sector Consultative Forum in April 2024 and through a public consultation in July 2024. The public consultation posed questions related to the involvement of the private sector in the NRA process, including best practices for requesting private sector feedback and outreach to private sector stakeholders on the findings of the NRA. The project team received 501 responses to the public consultation, from a variety of different sectors including financial institutions, DNFBPs, academics, non-profit organisations (NPOs) and consultants.

## Key Concepts Relevant to Assessing and Understanding ML Risks

Risk occurs when a threat successfully takes advantage of a vulnerability to produce a consequence. The below definitions explore how this relates to ML risk.

- A **threat**, in general, is a person, group or activity with the potential to cause harm to the state, society or the economy. In the ML context this refers to criminal individuals, groups or entities and their facilitators seeking to conceal the illicit origins of funds through past, present and future ML activities (and not the predicate offences themselves). The threat assessment typically serves as an essential starting point in developing an understanding of ML risk. For this reason, understanding the environment in which predicate offences are committed and proceeds of crime are generated to identify their nature, size and volume is important to carry out an ML risk assessment. In some instances, certain types of threat assessments might serve as a precursor for a ML risk assessment.

---

<sup>6</sup> Bahrain, Bhutan, Brazil, Canada, Cayman Islands, Caribbean Financial Action Task Force (CFATF) Secretariat, China, Eurasian Group (EAG) Secretariat, European Commission, Egmont Group, Finland, France, Greece, Inter-American Development Bank (IDB), International Monetary Fund (IMF), India, Ireland, Israel, Italy, Kyrgyzstan, Luxembourg, Portugal, Saudi Arabia, Singapore, South Africa, Spain, Sweden, United Arab Emirates, United Kingdom, United States, United Nations Office on Drugs and Crime (UNODC), Uzbekistan, World Bank.

- A **vulnerability** can be exploited by the threat or may support or facilitate its activities. In the ML risk assessment context, looking at vulnerabilities as distinct from threat means focusing on, for example, the inherent features of a particular sector, a financial product or type of service that make them attractive and feasible for ML purposes. Certain inherent characteristics of a country can also make it vulnerable to ML including a large financial, trade, or company formation sector. Vulnerabilities may also relate to a weakness in law, regulation, supervision, or enforcement. For example, deficiencies in AML controls, as well as non-compliance or partial compliance of national legislation with the requirements of the FATF Recommendations will impact the vulnerabilities in a country. Countries may include the adequacy or quality of AML controls in vulnerability assessment or focus their vulnerability assessment on inherent vulnerabilities and assess controls as a standalone component of ML risk.
- A **consequence** refers to the impact or harm that ML may cause and includes the effect of the underlying criminal activity on financial systems and institutions, as well as the economy and society at large. These consequences can be both domestic and international in scope, reflecting the far-reaching nature of ML activities. The consequences of ML may be short or long term in nature and relate to harm to populations, specific communities, the business environment and national or international interests. It can also undermine the reputation and attractiveness of a country's financial sector. Countries might focus on gaining a comprehensive understanding of their threats and vulnerabilities while considering the potential consequences as part of their overall risk assessment. This approach allows for effective prioritisation of mitigation efforts and helps in strengthening the resilience of financial and economic systems against the impacts of ML.

Other important key terms, relevant to conducting risk assessment are defined below.

- A **national ML risk assessment** is a process based on a methodology, agreed by all parties involved, that attempts to identify, analyse and understand ML risks and serves as a first step in addressing them. While assessments may take different forms, a ML risk assessment should cover threats (including predicate offences, characteristics of those committing predicate offences and ML offences) and vulnerabilities (including sectors, channels, geographic location, client type, products and services, deficiency or weakness of laws, regulations, supervision and enforcement) to come to conclusions about the risks at national level. The risk assessment should be a starting point to inform the national strategies and policies, development of an action plan and prioritisation of risk mitigating measures and resource allocation to strengthen the AML system in line with the risks identified.
- A **risk-based approach** (RBA) means that countries, competent authorities, financial institutions and DNFBPs identify, assess and understand the ML risk to which they are exposed, and take the appropriate and proportionate mitigation measures in accordance with the level of risk. This includes taking enhanced measures where risks are higher and taking simplified or lesser measures where risks are lower.
- **Risk mitigating measures** are actions, controls or strategies implemented to manage the identified ML risks. Risk mitigating measures can include legislative, regulatory, supervisory, law enforcement, or other administrative actions taken to mitigate risks within the national AML framework.

## Section 1: NRA Preparation and Set-up

While an NRA is, at its core, an analytical process, there are a few critical prerequisites that a country needs to have in place before beginning a successful NRA. The steps covered in this section are not explicitly covered by the FATF Standards but are necessary steps to undertake to perform what is required by the FATF Standards. They are not linear; they should all ideally be in place before the NRA begins. The critical prerequisites are covered in this section and include:

- i. Political Commitment to Conduct the NRA
- ii. An Inclusive, National Mechanism to Assess Risk
- iii. Appropriate Scoping and Objective Setting
- iv. Collection of Information and Data

There is no “one-size-fits-all” approach to the NRA, and countries are encouraged to take an approach that is appropriate to their capacity, risk and context. While countries should calibrate the NRA to their context, these steps remain prerequisites to a successful NRA regardless of the country’s capacity, risk and context.

### Political Commitment to Conduct the NRA

Political commitment to the NRA process is crucial for a successful risk assessment process. Political commitment demonstrates that the NRA is a priority for the country – senior government officials may publicly endorse the process and express their support for it, highlighting its importance and raising awareness among stakeholders. An indicator of strong political commitment can be seen when the NRA coordinator and/or working group are empowered and all experts involved in the process are given the appropriate level of autonomy and protection to do their jobs effectively.

Such support should help bring the right subject matter experts across policy, law enforcement, Financial Intelligence Unit (FIU), supervisory, regulatory, sanctions and other competent authorities together if they are not already collaborating on AML/CFT policies and priorities. It can facilitate and encourage coordination among the various government agencies involved in the process and improve information sharing, communication and collaboration.

High-level political commitment ensures that resources and budget are dedicated to the process across all involved agencies, to ensure NRA timelines are respected and to avoid excessive staff turnover that may disrupt the process. This can also include investment in technological solutions to facilitate parts of the process and improve consistency through future iterations. One example of this is investment in data collection tools, which can improve the accuracy and reliability of NRA findings and allows the country to not have to rely on external sources. Political commitment can also aid coordination and cooperation at an international level when conducting ML risk assessments.

### **Box 1. Statistics on High-level Political Commitment**

According to the responses received to the project questionnaires, many countries encountered challenges in coordinating the national risk assessment. Some of these issues raised by countries could be linked to a lack of political commitment at the highest levels, including lack of national coordination (35%), limitations in budget, resources or technical solutions (21%) and lack of commitment from those involved (9%).

In a survey by the World Bank<sup>7</sup> among a diverse group of country experts involved in NRAs, 9% of the respondents indicated that a lack of political commitment was a significant impediment to the quality of their NRA. In the same survey, according to more than 60% of participants, most significant challenges were linked to lack of political commitment, such as difficulties obtaining resources, coordination problems and lack of empowerment of the NRA working group.

### **An Inclusive National Mechanism to Assess Risk**

The FATF Standards require that countries should identify, assess, and understand ML risks at a country level by “designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are effectively mitigated.” The FATF permits flexibility for countries to adopt approaches to this based on their context and does not require the creation of a permanent body to develop the NRA. However, any chosen mechanism should promote good cooperation, coordination and participation of a wide range of national authorities to secure a comprehensive risk assessment. The most robust and effective countries demonstrate importance of regular meetings of those involved to make sure the NRA drafting is progressing in line with established timelines. Ideally, countries see the benefit of NRA processes and risk updates would be shared across participants even between NRA updates.

---

<sup>7</sup>. Figure.7,  
<https://documents1.worldbank.org/curated/en/099052110042330899/pdf/IDU0c1b39c8c0bfd604cf608ad40de3e4e0e24b8.pdf>

Table 1 shows some factors that countries can consider when setting up either a permanent or temporary NRA mechanism.

**Table 1. Factors to Consider: Permanent and Temporary Mechanism**

Permanent mechanism	Temporary mechanism
Promotes consistency and replicability across different iterations.	Gives for more flexibility in risk-based resource allocation, which is especially important for countries with lower capacity.
Helps foster good inter-agency coordination through building longer-term relationships with people and facilitating information sharing.	Allows countries that already have good inter-agency coordination to maintain it even in the absence of a permanent mechanism.
Allows participants to develop experience and knowledge in the NRA process and methodology.	Allows for other perspectives and points of view, makes sure the process does not stagnate and changes can be made, do not get "stuck in their ways".
Helps build institutional memory and expertise, making easier to assess the changes that have occurred throughout NRAs.	Can result in loss of expertise and disconnect with past risk assessments, especially if the staff turnover in agencies is high.
Ongoing overhead and cost.	

**Box 2. Mixture of Permanent and Temporary**

**Italy**

In Italy, the Financial Security Committee (FSC), comprising representatives of all relevant public authorities and administrations, maintains both a permanent coordination mechanism and a temporary dedicated team led by the Ministry of Economy and Finance. The permanent mechanism facilitates ongoing information exchange and monitoring, while the temporary team focuses on conducting risk assessments during NRA updates. This dual approach combines some of the benefits of a permanent mechanism in that it facilitates ongoing information exchange and monitoring, and the benefits of a temporary team in that it allows experts to dedicate their time towards shared goals over a short period.

Countries may choose to take a top-down or bottom-up approach to conducting the risk assessment, but often a combination of the two has been observed as being the most effective method for developing a comprehensive NRA. In a top-down approach, risk assessment begins with a high-level perspective and identifies broad categories of factors that may impact the country’s ML risks. It should be used to inform high-level strategies and actions such as budget allocation. A bottom-up approach relies more on industry level, sectoral and thematic risk assessment findings combined with the experiences of subject matter experts and operational level employees from competent authorities to inform the direction and scope of the NRA. It can help identify the likelihood of certain risk events occurring and support changes in procedures and controls at an operational level and identify key sector specific vulnerabilities. These approaches may begin to interact organically depending on the maturity of a country’s process and mechanisms.

***NRA Leadership***

Irrespective of the approach taken, countries should establish who will lead the process, whether it will be the responsibility of one agency or working group, or multiple agencies. Importantly,

countries should invest in leadership and find the right person/people to lead the process, ensuring they have necessary expertise in the FATF Standards, ML risk and the risk assessment process.

- Single agency or working group – Most countries that responded to the questionnaire identified their National AML/CFT Committee (or working group sub-set) as being the dedicated coordination authority to assess risks. Some countries cited the governing ministry or agency, for example the FIU, Ministry of Finance, or Ministry of Justice.
- Multiple agencies – Several countries cited more than one agency as having responsibility for leading the process. This requires strong coordination between agencies and a clear designation of roles and responsibilities, including procedures for decision making.

In considering whether a single agency/working group or multiple agencies constitute the NRA leadership, countries should also give regard to the individual(s) who will hold these leadership positions. These individual(s) require a cross-AML regime perspective, the ability to work with individuals from different competent authorities and the private sector and should have adequate seniority to inform senior policy makers of the process and its outcomes.

#### ***Involvement of all Relevant National Stakeholders***

A comprehensive assessment of ML risks will require involvement from key authorities across operational, policy and supervisory functions. The specific characteristics of the AML system will differ by country, including the mandates, objectives, powers and titles of the key operational authorities. Some key authorities include intelligence and security agencies, police, border security, prosecution authorities, the FIU, anti-drug authorities, anti-corruption authorities, customs, supervisory and regulatory authorities and foreign counterparts (i.e., national agencies in other countries). Regional authorities may also be involved, depending on the size and make-up of the country. Numerous other competent authorities may hold relevant information, including tax authorities, statistics departments and trade and commerce regulators. Depending on the country context, involvement of financial inclusion policy makers should also be considered.

The involvement of all relevant competent authorities is key to the success of the NRA process to foster strong national cooperation, several countries have established an interdepartmental and multi-agency NRA Committee to coordinate and integrate all relevant targeted national, sectoral and industry risk assessments. Based on Global Network responses to the project's questionnaires, it could be beneficial for a country to establish a defined decision-making forum, which has clear terms of reference, clearly outlining the roles and responsibilities of lead agencies and other participating entities. It could serve as a centralised body to oversee the NRA process, ensuring that it remains comprehensive, current, and reflective of the multifaceted threats the country faces. Additionally, the forum should delineate the decision-making hierarchy for various types of decisions, specifying which ones require escalation for consensus-building or for addressing divergent views.

Lastly, thought should be given to the diversity of NRA team itself, not only based on the agencies represented or professions of key constituents. Ideally, the team would also reflect age, gender, and identity diversity. This enriches the experience and knowledge base of the team and brings perspectives and ideas that may be otherwise be excluded.

### ***Involvement of Non-governmental Stakeholders***

While a ML risk assessment is an overall government assessment, countries should be encouraged to involve other non-governmental stakeholders with subject matter expertise, where appropriate. Such stakeholders and engagement may include, but is not limited to: FIs, DNFBPs, VASPs, civil society and academia. Some countries also include experts in risk assessment from outside of the AML world, and scientific or data experts to strengthen their approach to the NRA.

Involving non-governmental stakeholders can supplement or validate information from LEA and supervisors to detail what is occurring in practice. It also allows the consideration of private sector expertise on financial transactions, expertise about how products and services are used legitimately as well as misused for ML, industry practices and emerging threats. It can also help avoid an over or under generalisation of risk and prevent unintended consequences where the nuance of a certain product or sector are not more carefully considered.

Engaging non-governmental stakeholders can happen at any stage of the process — early, middle or end. Involving FIs, DNFBPs, VASPs, and civil society early in the process and on a continuous basis can mean the product is more impactful and useful to all stakeholders. Developing strong working relationships and building trust can ensure honest feedback and result in a willingness to share information.

Engaging with a representative sample from the sector (e.g., different services, different size of entity), including through the relevant supervisor is also important. Tailoring private sector outreach could be considered, as different approaches may be more effective depending on the size and maturity of each FI and DNFBP sector. Countries could engage non-AML specific industry bodies and work with them on how best to reach different parts of sectors and use their connections to give confidence that any responses they share with the NRA team will not be used against them in their supervisory assessments.

Countries may seek access to institutional risk assessments or other material from reporting entities or send out surveys or questionnaires to gain feedback and data. It is a good practice to have a standardised template to facilitate the analysis of the information received. Countries can also obtain input and feedback through interviews, roundtable sessions or meetings, and participation in public-private partnerships or other private sector forums.



### **Box 3. Involvement of Private Sector in NRA**

#### **United Kingdom**

In between NRAs, the UK hosts public private threat groups on priority areas that produce public-private threat alerts. Once the NRA process formally begins, the UK sends questionnaires to firms in the regulated sector to seek their perspectives on how the risks have changed since the last NRA. These are circulated via industry bodies, not AML supervisors, to give firms confidence that they can respond honestly, without risk of supervisory intervention.

Private sector contribution is also sought through NRA workshops with each sector. A diverse group of firms for each sector are invited (for example diverse in size and sub-sector) to engage in more detailed discussions on key themes from questionnaire responses. This includes areas where private sector views diverge from those of supervisors or law enforcement. The questionnaire and summaries of workshop discussions are included as one of the range of data sources used in drafting the findings of the NRA.

#### ***Ensuring the NRA Reflects Current Risks***

The FATF Standards require countries to maintain an up-to-date understanding of risks to take into account the evolving ML landscape. The Standards allow flexibility in how and how often this is done, recognising that countries should update in line with their risks, context, and capacity. Countries should take an RBA to updates in terms of schedule and scope and can prioritise high-risk themes or sectors for targeted updates or further study. Updates should be communicated in the same way as the NRA, to ensure a comprehensive and up to date understanding among stakeholders.

The NRA should not be regarded simply as a static document, but as a continuous process. While the analysis usually results in the creation of a formal NRA document, this document represents a snapshot of the country's risk situation at a specific moment in time. Countries should manage the NRA as a dynamic continuous process, constantly identifying emerging threats, managing residual risks and assessing the effectiveness of risk mitigation measures. This also allows findings from the previous NRA to be easily carried over into the new iteration. For example, some NRAs include an evaluation of the previous NRA and lessons learned to inform future NRAs, demonstrating that it is considered as an ongoing exercise.

While there is no requirement for countries to use data collected over a particular length of time in their NRA, data should span a sufficient time period and be current enough to provide an up-to-date, accurate and comprehensive view of its risks. This will vary depending on how frequently a country updates its NRA and if it conducts targeted updates and other risk assessment activities between NRA updates.

#### Box 4. Statistics on Timeliness of NRAs

The majority of countries (53%) that responded to the project questionnaire update their NRA every 2-3 years, and 27% update when there is a change in the risk landscape. The World Bank found that in practice, the average length of time between NRA updates in the countries they studied was 3.5 years.<sup>8</sup>

Some countries have legislation dictating the frequency at which they must update their risk assessment, and often there is a supplementary requirement to update the risk assessment if the risk landscape changes. The key is to have a mechanism that allows the country to take an agile approach that allows for quick adjustments to enhance risk understanding in case of changes to their risk situation, and to have ongoing discussions on a national level about risk, outside of any schedule they have for updating the NRA in legislation or otherwise. The statistics below emphasize the need for countries to see risk assessment as a continuous process that is constantly being reviewed, revised and updated.

#### Box 5. Statistics on Timeliness of NRAs

Research by the World Bank<sup>9</sup> found that completing the NRA too close to the on-site visit for the ME can limit the time available for risk-based policies to be introduced. According to the World Bank's study, of the 26 countries where this time span between completing the NRA and the onsite visit is three months or less, 17 had deficiencies identified in their risk-based national policies and strategies, which may imply that these countries had insufficient time to reflect the NRA results to national policies and strategies.

One benefit and purpose of conducting the NRA is to establish mitigation strategies or action plans with clear risk-based objectives and timeframes for implementation (discussed in detail in Section 3). The timing of the NRA and stage of the implementation of the risk mitigating measures based on the NRA findings materially affect the effectiveness of a country's AML framework.

### Scoping and Objective Setting

All parties involved in the NRA process should agree on the purpose and scope of the NRA before it begins. It is important to clarify from the outset the reason for conducting the NRA, the questions it should answer, the criteria that will be used to answer those questions and possible decisions that the NRA will inform. Countries should establish the target audience(s) early in the process and reflect throughout to guarantee the outputs are relevant for all stakeholders. They should also

---

8

<https://documents1.worldbank.org/curated/en/099052110042330899/pdf/IDU0c1b39c8c0bfd604cf608ad40de3e4e0e24b8.pdf>

9

<https://documents1.worldbank.org/curated/en/099052110042330899/pdf/IDU0c1b39c8c0bfd604cf608ad40de3e4e0e24b8.pdf>

consider that ML risk assessments should serve as input to a national AML strategy or strategies as part of the country's domestic AML co-ordination process.

The scope should be clearly defined and referred to throughout the process, and the country should ensure that it encompasses all relevant sectors, geographic areas, and illicit activities in line with the defined objectives. The scoping process also involves identifying the key stakeholders and determining the appropriate methodologies and data sources to be utilised. Effectively scoping the NRA ensures that resources and efforts are committed in a focused manner, thereby maximising the efficiency of the assessment.

### ***Actions to Take Before Starting NRA***

For countries with existing NRAs, a first step is to analyse the previous NRA and other risk assessment materials (e.g., thematic or sectoral risk assessments). Countries may find it useful to do this immediately after the NRA is published, while the information is still fresh in the minds of all stakeholders, or this exercise can be done as a handover note to future coordinators of the country's NRA. This feedback and direction will ensure that future NRAs are more robust and should answer:

- i. Process – Were the methodology and scope appropriate? Were there issues with data collection that could be resolved for the next iteration? Were all relevant authorities and other stakeholders involved? Did the country experience any difficulties developing risk understanding in the private sector? Were there any difficulties with the selection and implementation of risk-mitigation measures? Was there need for further alignment with national AML strategies?
- ii. Content and findings – e.g., Has the risk landscape changed and are there new threats and vulnerabilities to include? Which vulnerable areas have seen the introduction of risk mitigating measures? What data was lacking that could help draw conclusions on risk?

A good practice is to do a stocktake of available information and a gap analysis to see where data might be lacking. Stakeholder mapping is also useful for obtaining data at a national and international level. It is advisable to do this on an ongoing basis.

Many countries that responded to the project's questionnaires indicated that they took the following steps that yielded positive results:

- i. Studied the NRAs of neighbouring countries or supranational risk assessments (where available) before beginning their NRA.
- ii. Consulted experts from other countries that were rated highly or substantially effective on IO.1 in their MER.
- iii. Consulted reports from international organisations, news media other members of civil society, especially to identify new and emerging threats.

To keep the NRA process on track, countries should create a project plan with timelines, key milestones and deadlines throughout the process. Countries that have already undertaken an NRA can use lessons learned from their own experience, or that of other countries, to adjust their timelines for future iterations. The timeline should be based on the last experience building on the actual time spent by individuals and agencies on the various activities that make up the NRA process to develop more realistic and achievable timelines and goals. Tasks should be allocated to specific

people/departments and there should be an ongoing project monitoring mechanism to keep the process on track.

**Scope of NRA**

A key consideration when deciding on the scope of an NRA is to determine whether ML and TF risks should be assessed separately or together. More information to help countries make this decision is in Table 2 below.

**Table 2. ML/TF Assessed together or separately**

The risk of ML/TF is assessed together	ML/TF risk is assessed separately
Preventive systems in some countries are similar.	Different agencies and data sets are involved.
Allows countries to leverage collective ML/TF knowledge.	Different modules of the methodological tool are used.
More efficient when involving the same dataset.	Allows for greater flexibility when it comes to updating specific sections or delving into specific topics.

Source : Project questionnaire Responses – November 2023

**Box 6. Statistics on Scope of NRA**

The project’s questionnaires asked countries whether they assessed their ML and TF risks separately or together. 60% of responding countries conducted separate assessments, while 40% opted for combined assessments.

**Different Types of Risk Assessments and their Interactions**

The NRA should provide countries with a baseline understanding of their ML risks and help them to identify areas for policy focus. Many countries in the Global Network, undertake other risk-related work to supplement the findings of the NRA and develop risk understanding. Countries can also conduct sectoral risk assessments and thematic risk assessments, or other research related to risks to complement the information contained in the NRA, e.g., strategic analysis from FIUs, threat actor assessments by law enforcement or intelligence offices, thematic research from IFIs and independent research institutes and studies by supervisory authorities. Updating risk assessments in this way can involve fewer resources and less burdensome coordination with all agencies and stakeholders and allows for a "deep dive" into certain sectors, services or themes to gain a deeper understanding of risks. This allows a progressive approach to be adopted to promote more optimal use of resources, particularly in resource-limited or lower capacity situations.

Some international bodies such as the European Union (EU) and FSRBs have conducted supranational risk assessments identifying the ML risks across multiple countries or member states, which can assist countries when conducting their own risk assessment, especially concerning risks specific to the region and cross-border threats. Larger jurisdictions or those with overseas territories may also conduct sub-national risk assessments, which provide detailed information on a particular region within the country and can be particularly useful for border regions or other areas with certain characteristics that could make them more vulnerable to ML.

Countries should also consider the findings of risk assessment work done on an institutional level by FIs and DNFBPs, and other risk-related work done by the national authorities, e.g., trends and typologies reports.

Countries should aim to undertake risk assessment activities that complement each other as they all have distinct subjects, objectives and deliver different outcomes, as outlined in Annex A. They should also take an RBA, i.e., by prioritising highest-risk areas for sectoral/thematic risk assessments. It is important that these risk assessments are undertaken as part of the broader AML strategy to enhance the country's risk understanding as they become less beneficial when done in isolation.

A combined approach involving the development of an NRA which is supplemented by other kinds of risk assessment can help develop a more thorough understanding of risk among stakeholders. Including the findings of all risk assessments conducted in the NRA makes it more comprehensive and up-to-date and can support the implementation of more effective risk-mitigating measures. Countries can take the following actions to incorporate the findings into the NRA:

- **Standardising aspects of their risk assessments** – Countries should take steps to standardise methodologies and risk ratings to ensure that all risk assessments are comparable and easily integrated into the NRA.
- **Compiling data** – Compiling and integrating data collected in the development of the various risk assessments into a centralised, national level database gives a holistic view of data related to ML across different sectors, themes, countries and levels of administration.
- **Cross-referencing risks** – Doing a variety of risk assessments which involve different stakeholders allows the authorities to cross-check their understanding of risk in different areas and address any discrepancies. Do industry level risk assessment findings correspond with the findings of the sectoral risk assessment conducted by the government? If there are differences, the government can investigate why this might be (e.g., lack of private sector involvement in the NRA or change in risk landscape between assessments).

Ensuring that sensitive information is kept confidential throughout the NRA process is important for maintaining trust among all stakeholders and protecting information. Countries may have concerns about involving non-governmental stakeholders for confidentiality reasons. To combat this, countries can develop legal frameworks and procedures on the use and transfer of sensitive information during the NRA process and/or require that all participants sign a non-disclosure agreement. Countries should also have systems in place to protect data from unauthorised access, e.g., encrypted databases and communication channels.

Equally, countries may have concerns about involving non-governmental stakeholders based on a perception that such stakeholders may downplay risk or vulnerabilities to result lower levels of regulation. It is important to contextualise the information that's provided with other sources of information, such as that provided by LEAs, supervisors, intelligence information and the FIU.

## Collection of Information and Data

Data collection plays a role in every step of the NRA process, providing the necessary information to identify ML risk factors, forming the foundation for the subsequent analysis and evaluation. Data collection methods will depend on the size of the country, the quality of its national coordination and information-sharing mechanisms, and its capacity and resources dedicated to the process.

Data can be divided into two categories: quantitative and qualitative.

- **Quantitative data** refers to numerical, measurable information that can be expressed in terms of quantities or amounts. Quantitative data is important as it enables the drawing of objective conclusions based on numerical evidence. Examples include statistics on numbers of suspicious transaction reports received and disseminated, investigations, prosecutions, convictions, quantities of proceeds of crime confiscated, statistics on offenders, statistics on supervisory enforcement actions, etc. Quantitative information provides a good evidence base and ability to monitor trends, but lacks the contextual information needed to interpret the underlying causes and implications of the data.
- **Qualitative data** refers to non-numerical, descriptive information. For example, interviews with LEAs, supervisory authorities, and supervised entities yield mainly qualitative data. Case studies, expert opinions, and observations from various agencies including LEAs are also frequently used in NRAs. Existing typologies or trend analysis is also valuable. Qualitative data provides valuable insights into the perceptions, attitudes, and experiences of key stakeholders and helps in identifying gaps, weaknesses, and areas for improvement. Qualitative data can help explain the trends and patterns observed in quantitative data.

Both quantitative and qualitative data should be considered to provide a more accurate picture of the country's risks. For example, if no STRs have been reported by a sector it may appear as though that sector is low risk. However, qualitative information may tell us that a sector does not understand its reporting obligations or has only recently begun reporting, meaning the risks may be higher than the quantitative data would suggest.

Accuracy, consistency, and a critical approach to data sources are essential for effective data management and analysis in assessing risks related to ML. Below are several data considerations countries should consider:

- As it is likely that data is coming from a wide range of sources, it is recommended that information that overlaps is cross-checked to create the most accurate picture possible.
- Countries should also consider the level of confidence they have in the reliability of each data source and avoid taking data at face value. This process could help countries establish potential data gaps.
- Countries should ensure that the data they use is comparable and uniform over time periods, e.g., always using calendar year versus fiscal year.
- In cases where statistics may be limited – particularly in countries with few cases related to predicate offences or types of ML – countries should exercise caution. Even if statistics are available, the sample size and data quality may limit the statistical meaningfulness.
- A lack of data does not necessarily equate to a lack of risk and could indicate a heightened risk if it is indicative of a vulnerability within a country's AML/CFT framework.

Countries should keep track of areas where they have data gaps or procedural issues and improving these issues over time with each subsequent NRA. Developing a robust data collection process takes time and should not be rushed, as doing so could result in poor quality and misleading data.

Eighty percent of countries that responded to the project questionnaires indicated that they had experienced some challenges with data collection in the NRA process. Investing in a consistent and ongoing approach to data collection is important and can lead to resource savings in the long run as the process evolves and gets easier and quicker for each iteration. Countries should strive to use lessons learned from their NRA to improve and standardise their data collection processes. Some good practices for data collection from the Global Network are displayed below in box 7.

## Box 7. Good Practices in Data Collection

### Greece

In the context of the implementation of the national action plan to combat ML/TF, the National AML/CFT/CPF Strategy Committee established a Working Group for the recording of the statistical data required to be kept at the national level for the prevention and combating of ML/TF, and the evaluation of the mechanism.

The findings of the working group became the basis for a project to facilitate the digital collection of statistical data. Greece created a digital platform, in which the public authorities involved will register the statistical data that they maintain, and which relate to the prevention and suppression of ML/TF.

In this way, the Central Coordinating Authority of the MoF can automatically gather, the complete and updated statistical data kept by all competent authorities. The General Secretariat of Public Sector Information Systems of the Ministry of Digital Governance is the project promoter and provides technological support for the ongoing project which is funded by the EU Resilience and Recovery Fund.

### Finland

Finland employed a multifaceted approach to data collection for the 2023 update of the NRA, leveraging a Software as a Service (SaaS)-based risk management solution. This advanced platform facilitated the gathering of quantitative data from supervisory, legal, and enforcement authorities (a total of 17 organisations), as well as risk assessment questionnaires addressing individual sectoral risks and a comprehensive risk matrix. The software further enabled the easy analysis and visual presentation of the collected and analysed data, enhancing the overall efficiency and effectiveness of the NRA update process.

### The World Bank's Illicit Financial Flows Data (IFFD) Collection Tool

The World Bank's generic NRA Tool included a simple Excel template (Module 1.B) to help countries extract some key facts and figures from each money laundering case, such as the characteristics of each case (i.e. self-laundering vs. professional laundering, domestic vs. international), as well as sectors, products, assets, legal persons, and countries involved in each ML case. Considering the importance continuous collection of such data for understanding of proceeds of crimes, and ML risks, WB later developed a simple data collection tool for continuous and systematic data collection on proceeds of crimes and illicit financial flows in a jurisdiction. This tool aims to establish a proceeds of crimes data collection in countries. It helps building a national database of proceeds of crimes, generating statistics on main ML patterns and trends in the jurisdiction. The IFFD Tool is freely available to country authorities and researchers upon request.<sup>10</sup>



### **Data Sources**

Below is a list of data sources that can be used to inform the NRA, along with the information these authorities hold.

- **LEAs** play a critical role in combating money laundering by conducting criminal investigations and enforcing the law. They provide data related to predicate and money laundering offences, including the number of seizures and confiscations, published typologies, and statistics. While predicate offences often serve as the starting point for assessing money laundering threats, it is important to note that the threat also encompasses individuals committing the offence. Therefore, law enforcement data collection should also include insights from the criminals' perspective to understand their modus operandi and identify emerging trends.
- **Judiciary and prosecution authorities** provide data on judgements related to predicate and money laundering offences, as well as statistics on prosecutions and convictions. This data is essential for understanding the effectiveness of the legal framework and mitigation measures used in combating money laundering and terrorist financing and identifying areas for improvement. They can also provide cases which give more detailed qualitative information and provide useful context. The data from these authorities may also be helpful in assessing some geographic and demographic factors related to ML risks.
- **FIUs** play a pivotal role in the AML ecosystem by collecting, analysing, and disseminating financial intelligence. They provide valuable quantitative data such as Suspicious Transaction Reports (STRs)/ Suspicious Activity Reports (SARs), and qualitative analysis of transaction reports. Additionally, FIUs collaborate with other countries through MOUs to share critical financial intelligence and maintain statistics on formal and informal international information exchange. Frequently, they also conduct strategic analysis including produce reports on trends and typologies which should be leveraged during the NRA process.
- **Supervisory authorities** are responsible for overseeing the compliance of FIs and DNFBPs with AML regulations. They contribute qualitative data from both onsite and offsite examinations and other risk assessments including statistics on supervisory and enforcement activities. They also provide risk assessments that collect information on inherent risks and controls from regulated entities. Furthermore, they provide summaries of prudential and AML reporting requirements, and measures taken to mitigate ML/TF risks which offer insights into the regulatory landscape. The data from the supervisory authorities is also important to assess relative importance and materiality of sectors.
- **National security and intelligence agencies** often have access to sensitive information and intelligence that can provide valuable insights into emerging threats, transnational criminal networks, and evolving ML typologies. Their understanding of geopolitical dynamics and national security concerns can help

---

<sup>10</sup> [https://thedocs.worldbank.org/en/doc/3ea7ffa49269e00060ed6fb1a87507bb-0430012022/related/IFFD-Tool-Brochure.pdf?\\_gl=1\\*1wwez4\\*\\_gcl\\_au\\*MTUyNTQyNzUxNy4xNzI0NjA5OTM0](https://thedocs.worldbank.org/en/doc/3ea7ffa49269e00060ed6fb1a87507bb-0430012022/related/IFFD-Tool-Brochure.pdf?_gl=1*1wwez4*_gcl_au*MTUyNTQyNzUxNy4xNzI0NjA5OTM0)

identify ML risks that may arise from cross-border financial flows, sanctions evasion, and the exploitation of international conflicts.

- **National statistical agencies** offer quantitative data that provides a broader economic context for risk assessment. This may include data on the share of the economy attributed to specific sectors, national accounts, trade data, financial inflows/outflows, and other economic indicators that can help in assessing the potential scale and impact of money laundering and terrorist financing activities.
- Other governmental departments, including Customs, Tax, Immigration/Border Control, Fisheries, Environmental Protection, company registries, and Security Authorities offer data that may include information on cross-border movements, trade activities, and other activities that could be associated with ML.
- **Private sector** stakeholders can also provide detailed information on their experiences on the “front lines”. They can share information on trends that they see in their work that could lead to identification of new and emerging threats, and loopholes in regulation that may be exploited for ML.
- **Independent research and academic studies** can offer an objective, impartial perspective that can uncover vulnerabilities or emerging threats that may be under-reported or identify nuanced risks that may not be apparent from reviewing domestic data alone. Additionally, independent researchers can take a cross-jurisdictional view, highlighting ML trends and patterns observed internationally that could have spillover effects on the national risk environment. Countries should fact-check studies to ensure the findings are reliable and credible before using them as references.
- **International data sources, including NRAs and MERs from other countries in the region** provide valuable information on cross-border ML, corresponding predicate offences, and offenders. This data is essential for understanding the global nature of money laundering and identifying transnational threats. Other credible sources also include data from international bodies such as FATF, IMF, Interpol, OECD, UNODC, World Bank, International Organization of Securities Commissions (IOSCO), and regional bodies such as the Eurasian Economic Commission, European Commission, Association of Southeast Asian Nations (ASEAN), Europol, FSRBs.

### ***Data Challenges and Best Practices***

Obtaining up-to-date and accurate data for the NRA was mentioned by many countries across the Global Network as a challenge. They cited several reasons for this, including institutional capacity, lack of expertise on areas that are not reflected in crime statistics, and difficulties obtaining information from the private sector. Recognising these limitations, it is recommended that countries adopt a pragmatic and tailored approach to data collection and analysis that considers the specific context and constraints of each country. Countries cited some areas where they found it particularly difficult to obtain data, including on legal persons and arrangements, new and emerging technologies, unregulated and informal sectors, and lower risk areas. This section gives some more general guidance on supplementing insufficient data.

Where countries are facing capacity constraints that impact effective data collection and analysis, the following may be helpful:

- Prioritise data sources and focus on obtaining the most critical and relevant information can help mitigate the impact of capacity constraints on the NRA process.
- Collaborate with regional and international partners, leveraging existing networks and platforms, and seeking technical assistance and support from international organisations and development partners can also provide valuable resources, expertise, and guidance to support the NRA process and enhance the quality and reliability of the data collected.
- Use technological solutions, for example Artificial Intelligence (AI) programmes can analyse large volumes of data from different sources quickly and identify correlations and data anomalies that may not be immediately apparent. This can be used to supplement traditional methods and should always be interpreted by a subject matter expert. Investment in technologies help countries to build capabilities which can be used on a regular and ongoing basis, and also supports the continuity of the NRA process.
- Rely on subject matter expert consultations during the NRA process to identify specific barriers and propose solutions for data collection.

It is recommended that countries make every effort to develop and strengthen their data collection processes on an ongoing basis. However, this takes time. Some criminal activities and illicit fund flows may evade the purview of LEAs and official statistics and it can be challenging to assess and understand the risks associated with them without data. Understanding the potential size and nature of “unknown” threats and vulnerabilities allows countries to address blind spots and ensure the effectiveness of AML efforts.

Where countries find they are lacking data on a national level during the preparation of their NRA, they can take several steps to obtain more information to support their analysis:

- Leverage the expertise of national competent authorities by conducting interviews or consultations with them to supplement the data collected. Using targeted questionnaires can also be a rich form of information gathering.
- Access open-source information from publicly available sources, such as news articles, academic papers, reports from other countries and social media, to identify emerging trends, typologies, and methodologies in money laundering. Countries should always assess the reliability of such information and be conscious of possible bias and misinformation. This can give more context on the environment in which crimes are taking place.

## Box 8. Using Qualitative Data

### Montserrat

At the time of its NRA, Montserrat did not have robust data collection methods in place, and had to rely on external sources of data, e.g., neighbouring islands and international organisations for data, however limited international exposure with these counterparts limited the usefulness of the data.

In order to complement the data available to them, Montserrat requested information from public officials and private sector entities using questionnaires. Montserrat worked to build trust through transparent communication with all parties to ensure questionnaires were answered honestly, and to mitigate potential concerns surrounding data confidentiality and misuse within a small community.

This process helped Montserrat complement their limited domestic data to inform the NRA, but also encourages buy-in from all sectors for the NRA's follow-up actions and implementation of risk-mitigating measures.

- Consultation with Private Sector: Insights from the private sector and industry association experts can offer valuable information on the risks and vulnerabilities associated with specific sectors and products/services and contribute to a more comprehensive and nuanced understanding of the risk landscape.
- Field trips and physical assessments provide first-hand insights into the operational environment, activities, and vulnerabilities associated with specific sectors, industries, and regions, and help in validating and corroborating the data collected through other sources as well as providing context on sector/area specific issues. This could be particularly useful in border regions or free ports.
- Regional cooperation is also useful in sharing information between countries with a similar context and geography. Supranational risk assessments, NRAs and MERs of neighbouring countries can provide information on trends and typologies seen in the region.
- International data and information can be gathered in various ways, such as through participation in discussions at international meetings such as the FATF or by reviewing international typologies reports. Countries can engage in formal or informal international cooperation, sharing information through MOUs, bilateral/multilateral agreements or through organisations such as the Egmont Group of FIUs. This provides countries with a global context and can help identify emerging risks. Interactions with liaison officers during the ML risk assessment can also provide valuable insights.

### Box 9. “Unknown” Threats

#### Singapore

Singapore's FIU circulated a questionnaire to international counterparts from a range of countries including FATF members, countries in the region, and countries with which Singapore exchanges frequently. This questionnaire requested information regarding their perceptions on the following:

- Singapore's ML threats (including domestic and foreign predicate offences) and most vulnerable sectors.
- Typologies or modus operandi observed in Singapore.
- Feedback on LEA-to-LEA cooperation.

The responses were analysed, and findings shared with LEAs and supervisors, as discussed at Singapore's Risks and Typologies Inter-Agency Group to assess whether the results supported agencies' understanding of ML threats and risks based on other quantitative and qualitative information sources analysed by the authorities.

The findings largely corresponded with Singapore's own observations and helped to validate Singapore's understanding of its exposure to foreign predicate offences, its vulnerable sectors and perception of Singapore as a key source or destination of illicit funds.

Some countries have difficulty obtaining reliable or consistent information from the private sector. In these cases, countries have shown that the following steps can be helpful in encouraging engagement or help to obtain more information:

- Consult Suspicious Transaction Reports (STRs) for an overview of ML trends that the private sector is experiencing. Countries should be aware of potential for private sector biases whereby they may be more familiar with types of crime and/or their indicators that may give a false criticality to ML trends.
- Obtain inputs related to compliance and relevant vulnerabilities from supervisory authorities, rather than from the private sector entities themselves.
- Design standardised questionnaires that are clear, focused and concise. Lengthy surveys can lead to survey fatigue and low-quality responses. Using digital questionnaires and including closed-ended questions or constrained responses helps to promote data quality and consistency. Countries may wish to enlist the help of credible survey vendors or data specialists to ensure questionnaires are well-drafted and structured to facilitate data analysis and interpretation and maximise the utility of responses. Questionnaires could be tested on a smaller sample before they are distributed to target population.
- Consider public-private partnerships (PPP) to also provide more information to national authorities that they may not automatically have access to. Hearing from those working on the front lines can give an insight on the emerging trends in different sectors, types of transaction and customer, and key vulnerabilities.

- Participate in events and workshops with multiple private sector representatives to identify and gather information on cross-sectoral risks.

### **Box 10. Private Sector Engagement to Obtain Data**

#### **Germany**

Germany approached international academic contacts to discuss their methodology and potential ways to improve it. They also engaged national academic experts who had developed reports on the extent of ML activity in Germany, particularly on areas where they had gaps in data. When developing questionnaires to send to the private sector, Germany consulted a criminologist and sociologist to ensure that the structure of the questionnaire and wording of the questions would yield unbiased responses and facilitate the data analysis.

## Section Conclusion

**Table 3. Section 1 Key Points**

This table highlights the key elements of the preparatory stages of the NRA which are more specifically useful for countries at an initial stage of developing their NRA process.

	Key points
Political Commitment to Conduct the NRA	<ul style="list-style-type: none"> <li>• <b>Acquire senior government level commitment for the NRA</b> to bring together stakeholders across all agencies, promote empowerment of leadership and other participants, dedicate budget and resources and investment in the process, and obtain assurances of best efforts to implement any recommended actions from the findings.</li> <li>• On funding and resourcing:               <ul style="list-style-type: none"> <li>○ <b>Request support</b> from government budgets or external sources such as international development programmes.</li> <li>○ <b>Leverage international assistance</b> (several international bodies (e.g., Council of Europe, IMF, World Bank, UNODC) offer technical assistance and capacity building support and can provide resources, expertise, and training to support the development of the NRA).</li> <li>○ <b>Invest in certain core (but resource-intensive) activities</b> that are key to developing the NRA such as data collection, analysis and terms of reference to lay solid foundations for future iterations of the NRA; systematise some of these activities to the extent possible to facilitate certain parts of the NRA process.</li> </ul> </li> <li>• <b>Allocate existing resources strategically</b> by prioritising the NRA within the national AML strategy.</li> </ul>
An Inclusive Mechanism to Assess Risk	<ul style="list-style-type: none"> <li>• Create a mechanism that works for your country's context; it <b>does not need to be permanent</b>.</li> <li>• <b>Clearly define and formalise</b> leadership roles and responsibilities and institutionalise aspects of the NRA process to ensure replicability and sustainability.</li> <li>• <b>Plan labour requirements and NRA timeline in advance</b> – consult similar countries for workload estimates. Integrate NRA-related work into the work programme and objectives of officials involved in the assessments.</li> <li>• Build and maintain <b>institutional memory</b>.</li> <li>• <b>Involve all relevant authorities</b> across operational, policy and supervisory functions. Some will have a bigger role to play than others.</li> <li>• <b>Develop a coordination mechanism</b> between authorities to facilitate information sharing. Remove known roadblocks.</li> <li>• Clearly define and formalise <b>decision-making</b> processes.</li> <li>• <b>Maximise training/workshops/other outreach</b> for participants to establish a baseline knowledge of the FATF Standards, ML risk and risk assessments.</li> <li>• <b>Standardise risk terminology</b> to promote a consistent understanding among all stakeholders.</li> <li>• Engage with <b>non-governmental stakeholders</b> early and on an ongoing basis. Build trust with stakeholders.</li> <li>• <b>Use non-disclosure agreements</b> to maintain confidentiality of information.</li> <li>• <b>Minimize the time between completion of the NRA and its dissemination/communication</b>.</li> </ul>
Scoping and Objective Setting	<ul style="list-style-type: none"> <li>• <b>Ensure all participants agree on purpose, scope and target audience</b>. Decide the scope and format based on the risk and context of the country.</li> <li>• Before <b>beginning</b>, <b>review the findings and process</b> of the previous NRA. Draw relevant lessons on process and substance, i.e., identify what should be adjusted from last time.</li> <li>• <b>Do a stocktake of available information/data</b> to see where there may be gaps. Consult NRAs and MERs of other countries. Consult supranational risk assessments (if available) and institutional level risk</li> </ul>

	<p>assessment by FIs and DNFBPs.</p> <ul style="list-style-type: none"> <li>• <b>Develop a detailed project plan</b> with clear <b>deadlines</b> and deliverables. <b>Allocate responsibility</b> for each task.</li> <li>• <b>Undertake sectoral/thematic risk assessments</b>, prioritised based on risk, to complement the NRA and to update the country's risk <b>understanding</b> in a less resource-intensive way.</li> <li>• Take into account resource constraints and <b>availability</b> of technical assistance when choosing a methodology.</li> <li>• If using consultants or technical assistance providers, be aware of the risks of outsourcing too much of the process as they are not always familiar with the country's peculiarities in depth. <b>Ensure the national authorities remain fully responsible and accountable for the NRA process and implementing the findings.</b> The process should never be fully outsourced to external consultants.</li> </ul>
<p>Collection of Information and Data</p>	<ul style="list-style-type: none"> <li>• <b>Identify gaps in data throughout the process and work on collecting this data between NRA iterations.</b></li> <li>• <b>Prioritise data sources collected on a national level, while also gathering data at various sub-levels.</b></li> <li>• <b>Make use of other sources of information</b> (international sources, open-source, qualitative data from national authorities and reporting entities).             <ul style="list-style-type: none"> <li>○ <b>Leverage membership of international bodies</b> such as the FATF and FSRBs to takeaway good practices from countries with similar contexts and to enrich information on regional risks.</li> </ul> </li> <li>• <b>Invest in technological solutions</b> to help save resources in the longer term.</li> <li>• <b>Ensure all participants can access the necessary information.</b></li> <li>• <b>Use inter-agency MOUs</b> to facilitate information exchange.</li> <li>• <b>Establish appropriate mechanisms to incorporate intelligence agencies' inputs</b> in a secure way.</li> <li>• <b>Apply appropriate confidentiality protocols</b> to facilitate candid assessment.</li> </ul>



## Section 2: Assessing and Understanding ML Risks

The FATF Standards have made the assessment and understanding of ML risks foundational to an effective AML regime. R.1 requires countries to “identify, assess and understand” the ML risks they face, including designating an authority or mechanism to coordinate actions to assess risk, while INR.1 clarifies that countries should take steps to identify and assess their ML risks on an “ongoing basis”.

Once a country has put the critical prerequisites for a successful NRA in place as described in Section 1, it can begin the analytical process. There is no mandated or ‘one-size-fits-all’ approach for analysing national ML risks – a country should design a process considering its capacity, risk and context. This section suggests a linear approach to be taken by the country, but it is important to note that this is not a prescriptive tool. The steps outlined here represent collective input and good practices gathered from the FATF Global Network, but countries should adapt the approach to suit their own unique context and requirements.

The steps identified in this section to identify, assess, and understand the ML risks that the country is facing are as follows:

- i. Environmental Scan
- ii. Analytical Process
- iii. Analysis of Threats
- iv. Analysis of Vulnerabilities
- v. Risk Assessment
- vi. Horizon Scanning

### Environmental Scan

The country should begin the assessment of ML risks by conducting an environmental scan that considers the context in which the country finds itself, the threats its facing, and the vulnerabilities it may have.

#### *Considering the Country Context*

Each country faces a unique and differentiated risk of money laundering. It is useful to begin the process by first considering, on a relative basis, how much ML risk is the country facing, i.e., is the country generally a lower ML risk environment or a higher ML risk environment?

Such a determination can be deduced from the from a brief scan of the data that has been collected, context on the crime environment in the country, credible and reliable non-governmental information sources, as well as the intuition of the professionals that make up the team undertaking the NRA.

The purpose in undertaking such an initial exercise is to later test the assumptions that the country has made at the end of the process. For example, the ML risk level of the country should be reflected in the risk ratings attributed to the threats and vulnerabilities, just as the aggregate risk ratings of the constituents of a sector should be coherent with the vulnerability rating of the sector itself. If there are internal inconsistencies across the risk assessment process, countries should re-examine their process and conclusions to identify and resolve the inconsistencies.

### ***Identifying Threats and Vulnerabilities***

To complete the environmental scan, the country should develop an initial list of threats and vulnerabilities the country faces. The identification process should attempt to be comprehensive; however, it should also be dynamic in that new or previously undetected risks identified may also be considered at any stage in the NRA analytical process. Countries have identified the following good practices in making an initial determination on the threats and vulnerabilities that they face:

- i. **Regular Discussions among Stakeholders** – these discussions offer a platform for sharing knowledge, expertise, and perspectives on the latest developments in the money laundering and terrorist financing landscape. In some countries, designated conferences and workshops may be convened to facilitate experience sharing and collaboration among stakeholders. These conferences provide an opportunity for experts, practitioners, and policymakers to discuss emerging trends, challenges, and best practice. This may also take the form of standing working groups or regular, intra- and inter-agency meetings convened on certain threat topics.
- ii. **Engaging with Academia and Industry Experts** – this offers unique insights and perspectives on emerging risks and trends. Academic research, expert opinions, and studies can provide a deeper understanding of the underlying factors contributing to the evolution of ML activities, as well as innovative methodologies and approaches to combat these threats effectively.
- iii. **Taking Reference of LEA and FIU Observations** – their operational experiences and investigations can offer real-world perspectives on emerging crime trends, typologies, and modus operandi. By leveraging the expertise and intelligence gathered by LEAs, countries can gain a more comprehensive and accurate understanding of the evolving ML landscape. Regional reports of organisations such as Europol provide a broader perspective on the regional risk landscape, enabling countries to identify common trends, vulnerabilities, and areas for collaborative action.
- iv. **Leveraging Private Sector’s Inputs** – this includes FIs, DNFBPs, VASPs, industry associations, and other relevant organisations, and can provide valuable insights into emerging risks and vulnerabilities from a business perspective.
- v. **Monitoring International Developments, Trends and Typologies** – this includes the work of the FATF and the Global Network, as well as other credible sources. Reliable sources of information on ongoing conflicts, macro-economic trends, geopolitical dynamics, and potentially even natural/environmental changes will help frame and contextualise internally derived information, particularly as to predicate threats and threat actors.

Using these good practices, a country can arrive at a critical list of threats and vulnerabilities affecting it. Those involved in identifying threats and vulnerabilities must keep an open mind to ensure that all relevant factors are identified so as to avoid inadvertently overlooking key issues that contribute to the country’s ML risk. There should be no off-limit topics in the NRA brainstorm. The actual processes used to identify the initial list of risks will vary. Some countries may utilise more formal techniques such as surveys and quasi-statistical analysis of past events or circumstances, while others may carry out a brainstorming exercise among appropriate experts to produce a list or perhaps a tree diagram of related events or circumstances. It should be stressed that something identified on the list at this stage is not automatically classified as having higher (or

lower) risk – it has simply been identified as sufficiently relevant to go into mix of risks to be analysed.

Regardless of the process, the result of the country's environmental scanning should be a listing of threats and vulnerabilities that the country faces. Once an initial list is identified, the analytical process can proceed.

### Analytical Process

The analytical process is the critical part of the NRA. It is through analysis that the process moves from a description of the ML/TF risks facing a country to a complete understanding of the nature, extent and possible impact of the identified threats and vulnerabilities. The goal of this step is therefore to analyse the identified threats and vulnerabilities separately in order to understand their nature, sources, likelihood and consequences and then assign a relative value or importance to each (e.g., rating each on a scale of 1-10 based on their criticality).

The analytical process begins with the list of threats and vulnerabilities that has been developed by the country through the environmental scan. The next two chapters (Analysis of Threats and Analysis of Vulnerabilities) detail good practices first in the analysis of these threats and then secondly the analysis of those vulnerabilities. The analysis of threats and vulnerabilities should give regard to the likelihood, extent and consequence of money laundering that these threats and vulnerabilities would produce.

#### ***Consequence, Likelihood and Extent***

In assessing and assigning ratings for both threats and vulnerabilities, countries should consider analysing the likelihood and extent to which ML will occur, and the consequence that such ML will produce. If a country does not consider the likelihood and extent of the activity and the consequences it will have diminished ability to reach conclusions about their relative importance, severity and urgency of each assessed factor. These are key assessment factors.

There is no one-size-fits-all method for assessing the likelihood, extent and consequence of ML. Analytical techniques can involve identifying the nature and extent of the consequences of each threat and vulnerability along with the likelihood that the risk may materialise and combining those results to determine a level of risk, which is often presented through the use of a matrix. The actual process used to identify consequences and determine likelihood can also vary. Some countries may choose to employ more formal techniques such as surveys of experts or statistical analysis of the frequency of past ML risk related activity; others may choose to reflect on the conclusions of a group discussion or workshop to help develop this information. In the assessment of the consequences, it is also important to consider the cross-border consequences. Especially in international money laundering, most of the negative consequences may occur in foreign jurisdiction where the predicate crimes are committed and a consequence analysis that only focuses on domestic context (e.g., the effect on taxpayers) may not reflect the true scale of consequences. Destabilisation and skewing of markets, security impacts, the potential for misuse of domestic financial and non-financial actors, and the extent that its citizens may be victims of foreign crime are common consequences of cross-border ML for a country to contemplate.

## Box 11. Assessing Consequences

### Italy

In Italy threats' analysis also includes an estimate of consequences. Consequences are estimated using several parameters: financial estimate (measures the financial significance of the threat); legal penalty (measures the social disvalue attributed to the threat event); reports (measures the actual occurrence of the threat on the territory). Combining these parameters generates an indicator that supports experts in assessing threats.

### Sweden

In Sweden, consequence is analysed separately to threat and vulnerability. The National Risk Assessment of Sweden 2020/21 analyses the risk associated with each and every one of the sectors subject to Swedish AML laws. The first stage of the process required national agencies to provide data on threats and vulnerabilities. The parameters that comprise threat and vulnerability, as well as risk indicators, were used to assess threat and vulnerability linked to each sector across a four-grade matrix.

Then, consequences are determined by examining factors such as the size of a sector, its materiality for the financial system, public trust etc. The consequence and sectoral risk (a function of the threat plus the vulnerability) is then used to assess the societal or systemic risk. This helps policy makers and supervisory authorities to prioritise and take a risk-based approach, as well as helping obliged entities understand the consequences of large-scale ML in their sector.

Sweden found that separating the assessment of consequences from the initial analysis on threat and vulnerability allows the same data to be used at two levels of the analysis. The sectoral risks guide actors within the FI/DNFBP sectors to mitigate risks directly (e.g. through Know Your Customer (KYC) processes or Enhanced Due Diligence (EDD)). Systemic risks guide policy and law makers, as they must be mitigated through legislation, resource reallocation etc.

## Analysis of Threats

Fundamentally, a threat analysis aims to identify the main proceeds-generating offences that a country's systems are exposed to (i.e., predicate offences, both domestic and international) as well as the criminals perpetuating these offences (i.e., the perpetrators). Countries should analyse both predicate crimes and perpetrators as part of their analysis of threats for the ML NRA:

### *Predicate Crimes*

Countries should first identify the most prevalent predicate crimes driving ML activities within their contexts. This helps jurisdictions understand the severity of the threat and prioritise their efforts to address the most significant predicate crimes fuelling ML.

Countries should evaluate the scale and impact of the identified predicate offences. This involves analysing their prevalence by relying on domestic criminal, intelligence and FIU data such as: overall number of the predicate offences committed, proportion of the country's ML investigations, size of proceeds generated, STRs, prosecutions, convictions, asset seizures and confiscations, etc.

Interpretation of these figures requires caution due to various factors. For example, detected cases represents only a portion of the actual volume of crimes and there are always undetected crimes. The number of the detected crimes may be skewed by reporting behaviour. Crimes with direct victims (like robbery) are usually reported more, while some other crimes are under-reported (like human trafficking). Also, along the numbers of crimes, it is important to consider the total and average proceeds of crimes for each crime category. As a common example, the number of the theft cases will be much higher than any other crimes in most countries. However, this does not necessarily mean that property theft is the most important ML threat in the country.

Beyond domestic criminal data, countries should further rely on other sources of information and mechanisms to develop a more holistic overview, subject to a country's specific context and profile. For example, countries can establish a mechanism to identify their prevalent predicate offences, e.g., using quantitative data complemented by in-depth discussions or scoping exercises with LEAs, FIUs, sector supervisors, and consulting other relevant stakeholders to validate and refine their understanding of the key predicate crimes.

It is also important to understand how criminal proceeds being generated domestically can be laundered in the country or outside of it, as well as how illicit foreign proceeds are laundered in the country. With the increasingly transnational nature of ML, criminals are exploiting gaps in AML systems across countries to move illicit proceeds. Failing to account for these cross-border flows results in a substantially incomplete understanding of the actual risks. The examination of cross-border flows further minimises any impact of unknown unknowns. For example, high numbers of informal requests for information from a foreign country relating to a specific predicate could highlight domestic predicate threats that may otherwise be undetected.

### Box 12. Other Datapoints and Mechanisms for Threat Analysis

- Customs, immigration and tax data – These data provide valuable information on cross-border financial activities, customer profiles, and circumstances that can either facilitate or complicate cross-border transactions. Similarly, data on incoming and outgoing cross-border transactions across different sectors and international trade data can provide insights into the patterns, trends, and typologies associated with ML activities. For example, cross comparison of national trade records with trade partner countries can be very insightful for understanding trade-based ML (TBML) risks.
- FIUs and LEAs cooperation mechanisms – they can provide information on cross-border transaction analysis provides valuable insights into the risks associated with inbound and outbound suspicious financial flows. The analysis of such information makes it possible to identify trends and correlations with illicit and financial flows, which is an important element in understanding the overall picture of cross-border risks.
- Informal international cooperation requests - Leveraging Interpol and Egmont requests and other international informal requests and data can provide insights into international investigations, intelligence sharing, and collaborative efforts to combat transnational organised crime and illicit financial flows. Some countries may have designated teams or units established to study specific topics or set up teams in overseas offices to facilitate intelligence exchange and cooperation with different sectors, such as Virtual Asset Service Providers (VASPs) and credit card businesses.
- Formal international cooperation requests - Leveraging Mutual Legal Assistance (MLA) information and other forms of formal international cooperation data can also enhance their capacity to identify invaluable insights into the cross-border aspects of ML activities, filling the gaps in identification of predicate offences occurring outside the country.

### *Perpetrators and Typologies*

It is useful to develop a comprehensive understanding of the perpetrators involved in predicate and ML activities. Perpetrators can range in different levels of complexity, and can include organised crime groups, white-collar criminals, corrupt officials, low-income groups employed as money mules, among others.

A collaborative approach with LEAs, FIUs, and other relevant stakeholders can be useful to gather intelligence across various sources and develop comprehensive profiles of the ML perpetrators. In cases of transnational organised crime groups, engaging foreign partners can promote a common and robust understanding. Authorities can also examine the specific ML techniques and typologies employed by different perpetrators.

### Box 13. Understanding typologies

#### Brazil

Brazil's 2020 NRA methodology included a study of ML/TF typologies, which sought to reinforce the analyses made in the assessment of threats and vulnerabilities, identifying "how" (i.e., by which means, structures, formats and arrangements) threats have carried out their operations in the country and which sectors and control systems may be affected.

Based on a list of 62 previously identified typologies, several institutions in the AML/CFT system have been invited to contribute with other operation methods, which are possible, relevant, and recurring, but still not formally identified. The final product of this process, in addition to its use for the purposes of the NRA, was published in collaboration with COAF in a document titled Cases and Cases – Collection of ML/ Countering the Financing of Terrorism and Proliferation (CFTP) Typologies, Special Edition, National Risk Assessment, 2021, aiming to promote the dissemination and raise awareness in the AML/CFTP community.

Ultimately, such an understanding of perpetrators and typologies is useful in allowing authorities to evaluate the technical expertise, resources, and networks available to perpetrators. Increased criminal proficiency may suggest a need to look deeper into hidden networks and unknowns are minimised to develop a holistic threat understanding.

#### ***Cross-border ML Threats and Foreign Predicate Offences***

Assessing domestic ML threats also includes understanding the role of a country as a generator of criminal proceeds that are laundered domestically or abroad, as well as how foreign proceeds are laundered in the country.

ML methods can evolve quickly on a global scale, and vulnerabilities in one country can be exploited by criminals in others, undermining domestic control efforts. Failing to account for these cross-border flows results in a substantially incomplete understanding of the actual risks, and ignoring cross-border trends can mean a country lacks the ability to detect emerging threats. Underestimating the impact of transnational money laundering can significantly undermine the effectiveness of country, regional, and even the global AML framework. Countries should therefore adopt a balanced approach that thoroughly examines both the domestic ML landscape and ML vectors to and from foreign countries, by evaluating international and cross-border risks as part of a comprehensive NRA.

Cross-border ML includes the risks of both incoming and outgoing ML flows, posing challenges in gathering data on the proceeds of crime and associated predicate offences. Considering the increasingly cross-border nature of ML and financial crime, international collaboration has become critically important in conducting the NRA, enabling coordinated efforts to disrupt transnational ML networks.

Identifying overseas predicate offenses, which are the underlying criminal activities generating illicit proceeds, is particularly important in assessing cross-border ML threat. But this can be challenging due to the complex and transnational nature of these crimes. Drawing from comprehensive studies from the Global Network, some good practices have been identified to navigate these challenges.

### Box 14. Good Practices in Assessing Cross-border ML Threats

- Consulting foreign government partners – this provides useful insights into prevalent predicate offenses in foreign jurisdictions. By collaborating with these partners, countries can gain a better understanding of the nature, trends, and characteristics of overseas predicate offenses, enabling them to develop targeted strategies and interventions effectively. For example, Singapore, Indonesia and Malaysia proactively engage their domestic and global counterparts or regional; consultative group by way of surveys, to obtain feedback as additional data points to competent authorities' assessment and understanding of their ML threats and vulnerabilities related to cross-border crimes or foreign predicate crimes and laundering offshore and the associated illicit fund flows. By establishing and strengthening partnerships, sharing intelligence and best practices, and collaborating on joint investigations and operations, countries can enhance their capacity to identify, investigate, and disrupt ML networks, and recover illicit assets.
- Engaging with a diverse range of stakeholders – these include journalists, academics, and industry experts, who can provide deeper insights into the broader societal, economic, and political factors influencing ML activities. Some countries conducted focus group discussions with stakeholders to gain insights on issues, trends and modus operandi associated with illicit fund flows, as well as identifying potential foreign elements and transnational connections involved in ML activities. This engagement aids in developing a comprehensive understanding of the ML landscape and devising targeted strategies and builds partnerships.
- Regional collaboration platforms – in some regions, neighbouring countries have established communication protocols to share updates on prevalent predicate offenses. For instance, in the Nordic countries and the Tri-Border area in South America, such protocols facilitate the exchange of information and intelligence regarding emerging trends, typologies, and developments in predicate offenses. Leveraging these established communication channels can enhance cross-border cooperation, intelligence sharing, and joint investigative efforts, thereby strengthening the capacity to identify, investigate, and disrupt money laundering networks.

### ***Drawing Conclusions on Threats***

After bringing together and considering the various quantitative and qualitative data, countries will need to contextualise and assign a rating to the threats assessed. Countries vary in how they assign a threat rating, and there is no hard and fast rule. The threat ratings should be assigned on a relative basis, providing the country with an indicator of which predicate offences and perpetrators pose the greatest threat and, therefore, where AML efforts and mitigating measures should be prioritised. This could be done, for instance, on a scale of 1-10 with qualitative descriptors defining each of the threat ratings. The descriptors for each rating should include the likelihood and extent to which the threat is involved in ML in the country, and the consequence of those ML activities. Such a standardised approach that identifies the criticality of threats allows for objective, useable results that can contribute to the post-assessment actions, as detailed in Section 3 of this guidance.



The threat assessment should document the ‘why’, i.e., why was the threat assessed to have reached a criticality or rating level. This documented rationale provides the ability for policy makers and operational authorities to take post assessment actions, as detailed in Section 3 of this guidance.

### **Analysis of Vulnerabilities**

A vulnerability can be exploited by the threat or may support or facilitate its activities. In the ML risk assessment context, looking at vulnerabilities as distinct from threat means focusing on, for example, the inherent features of a particular sector, a financial product or type of service that make them attractive and feasible for ML purposes. Fundamentally, an analysis of vulnerabilities aims to identify the main sectors, products, services, channels, customer bases, geographical locations, and other national-level factors (including weaknesses in systems, controls, or mitigation measures) that threats are most commonly exploiting for ML activities.

Countries should consider examining vulnerabilities at both the national and sectoral levels. Integrating both national and sectoral perspectives into the risk assessment process ensures that countries develop a comprehensive strategy to mitigate ML vulnerabilities and safeguard the integrity of the financial system. By assessing national level vulnerabilities, the holistic assessment will help identify systemic gaps or weaknesses that could be exploited by money launderers. On the other hand, by examining sector-specific vulnerabilities, countries can gain a nuanced understanding of the unique ML landscape and prioritise targeted interventions to strengthen the resilience of high-risk areas.

#### ***National Vulnerabilities***

When assessing ML vulnerabilities at the national level, authorities could evaluate vulnerabilities related to AML controls, including comprehensiveness of the country’s legal and regulatory framework for AML/CFT. Deficiencies in the national AML framework may provide critical vulnerabilities for criminals to exploit. This includes reviewing the breadth and depth of the applicable laws, regulations, and guidelines, as well as their alignment with international standards. It also has an impact on the effective coordination, resourcing, capacity and effectiveness of the national authorities, examining the availability of specialised training, access to technology and financial intelligence, and the ability to effectively detect, investigate, and disrupt ML activities.

A candid and unbiased examination is key to the national vulnerability assessment. Reference may be made, for example, to outside assessments of the country, but internal, critical, and open-minded self-reflection is required, without regard to political implications, the messaging of industry, or the likelihood of future mitigation. Institutional biases should be considered and known weaknesses (e.g., documented corruption within law enforcement or a lack of independence in the judiciary) should be acknowledged (and potentially adapted to) in the NRA process. Even vulnerabilities considered historical in nature might be re-examined with fresh eyes.

Apart from vulnerabilities related to the AML controls, some vulnerabilities may arise related to inherent factors in the country, such as the size and complexity of the economy, size and geographic spread of financial services, the extent to which the economy is informal/cash based, or the diversity of legal persons and arrangements. On this note, the impact of financial exclusion on the size and risk of the informal/cash-based economy should also be considered. Social factors such as immigration, social cohesion and areas of conflict in the population can be noted, as well as the use of technologies in financial transactions and geographical factors.

### ***Sectoral Vulnerabilities***

Alongside the national-level evaluation, a comprehensive ML vulnerability assessment should cover the examination of the inherent vulnerabilities associated with different financial and non-financial sectors within the country, including FIs, DNFBPs and VASPs. Each sector will likely present unique vulnerabilities that money launderers may seek to exploit, and a targeted, sector-specific analysis is essential for developing effective countermeasures. Certain sectors may offer products or services with higher-risk features. Common features of high-risk sectors involve a high volume of cash transactions, cross-border funds movement, or the ability to obscure beneficial ownership, making them attractive for money launderers.

Sectoral assessment could evaluate the level of compliance with existing AML obligations, such as customer due diligence, transaction monitoring, and suspicious activity reporting. The assessment should also examine the level of integration with other regulated sectors. To take an example, the quality and availability of beneficial ownership information available to the entities operating within these sectors may be an influential factor. The assessment of compliance-related vulnerabilities should be based on findings of supervisory activities, rather than self-reporting by the private sector.

Moreover, the sectoral vulnerability analysis should consider the effectiveness of AML supervision and enforcement mechanisms for different industries. Weaknesses in the supervisory regime, such as insufficient resources, lack of specialised expertise, or inadequate sanctions for non-compliance, can create vulnerabilities that money launderers may exploit.

As reported by several countries, the lack of information about and from certain sectors poses challenges in assessing their vulnerabilities. Engaging with the private sector early in the process, and on an ongoing basis, can help countries clearly set out their role and the input expected (e.g., data specific to the sectoral landscape, observations on suspicious transactions, modus operandi of offenders).

Finally, the existence of entirely unlicensed and/or unregulated sectors, or illegal segments of regulated sectors, should be considered as an overarching factor in the sectoral vulnerability analysis. Failure to note the existence or possibility of unsanctioned financial services undermines the entirety of the vulnerability analysis portion of the NRA. Often the regulated and would-be competitors of such rogue service providers would be in a position to point to unlicensed operators, another point in favour of a close dialogue with the private sector (particularly including small to mid-size operators within the sector who may be more likely to face pressure from illegally operating businesses). Supervisors will also be attuned to this vulnerability but may not be tasked specifically with looking for it. The presence of informal businesses or “off the books” services of otherwise regulated businesses might be more prevalent in the Money or Value Transfer Services (MVTs), money exchange, Trust and Company Service Provider (TCSP), gambling, and VASP sectors, to name a few examples drawn from country input. It is also possible that unlicensed services may be utilised by specific communities or groups or be more common in certain geographic locations within the country. Additionally, NRA teams should practice scepticism of claims or long-held assumptions that certain sectors ‘do not exist’ in the country or are fully banned by domestic law or regulation, recalling that services may be offered online within a country even if they are hosted offshore.

### ***Drawing Conclusions on Vulnerabilities***

After bringing together and considering the various quantitative and qualitative data, countries will need to contextualise and assign a rating to the vulnerabilities assessed. Countries vary in how they assign a vulnerability rating, and there is no hard and fast rule. The vulnerability ratings should be assigned on a relative basis, providing the country with an indicator of which national areas, sectors and products/services should have mitigating measures and should be prioritised. This could be done, for instance on a scale of 1-10 with qualitative descriptors defining each of the vulnerability ratings. The descriptors for each rating should include the likelihood and extent to which the vulnerability is exploited for ML in the country, and the consequence of those ML activities. Such a standardised approach that identifies the criticality of vulnerabilities allows for objective, useable results that can contribute to the post-assessment actions, as detailed in Section 3 of this guidance.

#### **Box 15. Weighting of Sectors**

##### **World Bank**

Once vulnerabilities of various FI and DNFBP categories are assessed, the World Bank's NRA Tool offers two approaches to users for determining the overall vulnerability from all sectors:

1. **Economic Importance-Based Weighting:** This method requires the NRA working group to assign weights to each FI and DNFBP category on a scale from 1 (Very Low) to 10 (Very High), reflecting their significance in the country's economy. As sectors vary widely, no single indicator is universally applicable. For instance, while the banking sector may be gauged by total asset size, this measure is less pertinent for sectors such as money transfer businesses, insurance, real estate, or lawyers. Consequently, the World Bank advises using multiple indicators—including asset size, GDP contribution, annual turnover, employee count, and client base— together to determine relative weights. The country's overall sectoral vulnerability is then calculated using a weighted average of sector-specific vulnerability ratings.
2. **Vulnerability-Based Weighting:** In this approach, sectors with greater vulnerabilities carry more weight in the overall vulnerability rating. Such weighting prioritises the top 20 percentile of sectors based on their vulnerability ratings and uses their average to compute the overall sectoral vulnerability, yielding more conservative results. This method is also known as the "open door approach," with a reference to the risk to a house with all but one entryway secured, highlighting the potential for risk through the least protected area.

The first method is the tool's default and is widely utilised by countries. Users can select either approach to represent overall vulnerability or analyse it as a band between the two levels. This weighting can be done for sectoral risks (rather than vulnerabilities), which is preferred more in recent applications of the NRA Tool."

While a structured, data-driven approach can provide a useful starting point, the vulnerability assessment process should ultimately involve a more comprehensive, contextual analysis that considers the unique circumstances and interdependencies within the jurisdiction. Countries should leverage professional judgment and discretion. The final vulnerability rating should reflect a holistic, evidence-based assessment that incorporates the unique context, interdependencies, and evolving dynamics within the jurisdiction.

The vulnerability assessment should document the ‘why’, i.e., why was the vulnerability assessed to have reached a criticality or rating level. This documented rationale provides the ability for policy makers and operational authorities to take post assessment actions, as detailed in Section 3 of this guidance.

Materiality is an important factor in the vulnerability assessment, however, determining relative “weight” can be challenging. Engaging with supervisory and regulatory authorities is vital to gather data on the quality and effectiveness of AML systems. This includes information from on-site inspections, thematic inspections, and the evaluation of the vulnerabilities and inherent risks associated with ML, as well as using quantitative indicators such as business size and transaction volumes.

## Risk Assessment

Inherent risk is the extent of risk present without the consideration of any risk mitigation measures; residual risk, on the other hand, does take into account the impact of a country’s mitigation measures.

### *Inherent Risk*

Inherent risk is defined as the level of risk that exists before introducing any mitigating measures. This should be the starting point for countries when conducting a risk assessment.

The goal of an overall risk assessment is to determine how threats may interact with vulnerabilities to develop the final risk understanding. Countries can use different approaches to analyse risks and formulate the risk rating, such as a risk matrix, heat maps, or a mathematical or statistical formula to rate the final levels of risk. While there is no single, definitive model, those involved in the risk analysis might collectively rank or categorise each of the identified risks in terms of their degree and relative importance.

In many instances, exploring the intersection of how threats and vulnerabilities interact will not lead to any (material) change in the relative importance of the threats and vulnerabilities (i.e., if a vulnerability was assessed an importance of 7/10, then it generally remains as such). But this analysis of the interaction is critical for risk understanding, as it provides a more granular understanding of the risk environment in the country.

### *Residual Risk*

Residual risk is defined as the level of risk that remains after risk mitigation measures have been introduced.

The NRA could include the assessment of existing risk mitigating measures. These can include the existing policy and operational measures that the country is taking, as well as the degree of compliance by FIs, VASPs and DNFBPs, the efficacy of suspicious activity reporting, and the impact of supervisory actions taken by the relevant authorities. The level of maturity and embeddedness of certain mitigating measures and known effectiveness challenges of mitigating measures taken in

the past, could be factored in (i.e., a new beneficial ownership registry or new cash reporting requirement may not yet have anticipated impact for several years). Accordingly, residual risk is lower than or at most equal to the inherent risk depending on the quality of controls implemented to mitigate the risk.

This detailed analysis sheds light on the extent to which the existing risk-mitigation mechanisms are being effectively implemented and whether they are achieving the desired outcomes in detecting, deterring, and disrupting ML activities. This gap analysis serves as the foundation for considering further risk mitigation measures, or simplified measures, as described in Section 3 of this document. Countries are encouraged to engage with stakeholders such as supervisors, the private sector, civil society etc. on the impact of the mitigating measures on their work.

### **Box 16. Determining the Risk Rating**

#### **Hong Kong, China**

Hong Kong, China runs stakeholder workshops at the outset of each NRA exercise to explain the NRA methodology and the assessment criteria of each key ML risk component to ensure an aligned and agreed understanding of the methodology and the rating standard. Initial ratings of risk components and the justifications are discussed among stakeholders and agreement reached on a consensus basis, which form the foundation of the subsequent review and formulation of risk mitigation measures.

Having analysed the inherent risk profile which incorporates the evaluated consequences and likelihood of money laundering activities and provides a holistic perspective on the jurisdiction's overall risk exposure, Hong Kong, China then considers the various risk mitigation measures in place. This determines the residual risk components that remain after accounting for these risk-mitigating factors. A heat map that shows the intersection of the threat and vulnerability levels is used to present the final risk rating. The risk rating is then shared and discussed in the Steering Committee, where all relevant stakeholders join to review the findings, provide feedback, and collectively agree on the final risk assessment. This collaborative approach ensures the risk rating is fair, reasonable, and commonly accepted, setting the stage for the development of targeted risk mitigation strategies.

#### ***Validating Results***

As part of the first step in the process, the country considered whether it had a higher or lower ML risk in aggregate. Now that the country has evaluated the component parts that make up ML risk, that is the threats, vulnerabilities and consequences, the results bear consideration. If the country considered itself to be at a relatively lower risk of ML but had a number of threats and vulnerabilities rated highly, this should prompt some consideration by the country as to whether they are truly at lower ML risk on aggregate. Equally, if a country considered themselves to be at a higher ML risk than other countries, but had fewer threats and vulnerabilities rated highly, then they should consider whether they have assessed the threats and vulnerabilities for the country in the appropriate manner.

The risk assessment process should be coherent across different levels of risk analysis, i.e., the ML risk level of the country should be reflected in the risk ratings attributed to the threats and vulnerabilities, or the aggregate risk ratings of the constituents of a sector should be coherent with

the vulnerability rating of the sector itself. If there are internal inconsistencies across the risk assessment process, countries should re-examine their process and conclusions to identify and resolve the inconsistencies.

### Horizon Scanning

Finally, countries should attempt to stay aware of developing and emerging threats, vulnerabilities and risks to bolster their preparedness and adapt to the evolving risk environment. This materialises in two ways: (1) understanding the trajectory of the threats, vulnerabilities and risks, and (2) identifying emerging threats, vulnerabilities and risks.

Understanding and anticipating new and evolving risks within the dynamic landscape of financial crimes can pose significant challenges. It necessitates ongoing monitoring, collaboration, and the utilisation of diverse intelligence sources to gain a comprehensive understanding of the threat and vulnerability landscape. It involves examining emerging criminal groups, new products and services, and other factors that may contribute to a change in the risk environment, including the effects of mitigation measures. For example, legislative or regulatory measures implemented in one sector may displace money-laundering activities to another sector. Understanding these dynamics and their potential impact on the risk landscape is crucial to developing proactive and adaptive strategies and measures. Many countries employ horizon scanning to identify potential drivers for money laundering and areas of risk.

Although the emerging threats, vulnerabilities and risks examined in horizon scanning may not yet be critical enough to be part of the analytical component of the money laundering NRA, countries should document their observations and how these factors currently impact the risk environment. This documentation will ensure that future iterations of the NRA consider these emerging risks or are addressed in other analytical efforts between NRAs.

Countries should also strive to stay abreast of the trajectory of threats, vulnerabilities, and risks during the activities outlined in the previous sections. This will give the NRA a future-looking component and could identify threats, vulnerabilities and risks which may become more prevalent in the near future. These hypotheses of trajectories should be tested on an ongoing basis if risks are expected to reach a critical level.

### Box 17. Horizon Scanning

#### Australia

Australia utilises strategic intelligence methodologies and techniques which are used by Australian law enforcement and intelligence agencies to assess the trajectory of predicate crimes and sectors/channels, enabling the identification of emerging threats and proactive measures. The near term (three years) trajectory of each predicate crime and sector/channel was assessed as either increasing, emerging, stable, or decreasing.

One threat that was analysed in Australia's 2024 ML NRA was scams, in particular the evolving nature of scam methods due to perpetrators' more sophisticated use of technologies. It was noted that criminals leverage the growing number of customers interacting through digital channels to be able to reach more victims more efficiently, for example through impersonating phone numbers, email addresses or websites of legitimate organisations, or creating fake adverts, social media profiles and reviews. Australia concluded that this threat is likely to increase over the next three years and will be becoming increasingly challenging to disrupt given criminal use of technology and artificial intelligence.

#### Denmark

In Denmark's 2018 NRA, there is a section dedicated to future crime trends. All four activities identified were cybercrime-related threats, all conducted via the internet. One of the threats identified was hacking and espionage, rated as high risk. Denmark noted that the most popular methods were DDoS and ransomware attacks. At the time of the NRA, Denmark had only experienced such attacks that involved identity theft or blackmail. It used a variety of sources to develop the assessment, for example: demographic and economic trend data from Denmark's national statistics department, international data on digital payment solutions and digital banks, data on Denmark's Financial System from IMF, information about encryption from Europol.

Based on this, Denmark concluded that the increasing sophistication of technologies could put human lives in danger, and emerge more in economic crime, having an impact on the ML risk landscape.

## Section Conclusion

**Table 4. Section 2 Key Points**

This table highlights the key elements of the analytical stage of the NRA.

Sub-section	Key Points
Environmental Scan	<ul style="list-style-type: none"> <li>• <b>Consider the particular context of your country</b> when conducting the NRA to identify particular themes that may need closer attention - e.g. geographical, political, economic, structural, social/cultural, technological, and legislative factors can impact ML risk.</li> <li>• Develop an initial view of the <b>country-level ML risk level</b>.</li> <li>• Identify a list of the most critical ML threats and vulnerabilities affecting the country. In this exercise, utilise critical self-reflection and jettison pre-conceived notions and biases.</li> </ul>
Analytical Process	<ul style="list-style-type: none"> <li>• Develop a structured process to analyse the <b>scope, nature, likelihood and consequence</b> of the identified threats and vulnerabilities.</li> <li>• Through the process, provide a <b>relative assessment of the criticality</b> of threats and vulnerabilities, i.e., low, medium, high-level threat.</li> </ul>
Analysis of Threats	<ul style="list-style-type: none"> <li>• Consider the crimes leading to money laundering in the country, and the perpetrators committing laundering the proceeds of their crime.</li> <li>• Recognise domestic and cross-border threats.</li> </ul>
Analysis of Vulnerabilities	<ul style="list-style-type: none"> <li>• Consider national and sectoral level vulnerabilities.</li> </ul>
Risk Assessment	<ul style="list-style-type: none"> <li>• Explore the interaction between threats and vulnerabilities affecting the country.</li> <li>• Validate results to ensure that the <b>risk assessment is internally coherent</b>, i.e., the ML risk level of the country should be reflected in the risk ratings attributed to the threats and vulnerabilities, or the aggregate risk ratings of the constituents of a sector should be coherent with the vulnerability rating of the sector itself.</li> </ul>
Horizon Scanning	<ul style="list-style-type: none"> <li>• Attempt to understand the <b>trajectory of threats and vulnerabilities</b>, i.e., are certain of these becoming more serious over time.</li> <li>• Engage with public and private stakeholders to <b>identify emerging risks</b>.</li> </ul>



### Section 3: Post-NRA Actions

The FATF Standards clearly demonstrate that the identification, assessment and understanding of ML risks is purpose-drive. INR.1 indicates that “Countries should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country’s AML/CFT regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.”

Further, R.2 identifies that, “Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively”.

The purpose of the development of a granular understanding of national ML risks is to tailor national AML strategies to that risk. Tailoring AML strategies to risk means that areas of higher risk should be subject to enhanced risk mitigation measures. This is, however, an incomplete implementation of the risk-based approach. Lower risk areas should also be subjected to simplified or lesser measures.

An important goal of the NRA is to ensure that all relevant stakeholders fully understand the ML risks the country is facing and take effective measures to mitigate them. The dissemination and communication of the NRA results represents an important milestone in the process. However, it is essential that the NRA process is seen as continuous, and the NRA document is viewed as a snapshot of the current ML risks in the country based on an appropriate method of evaluation according to the country's context.

Lastly, the risk environment faced by a country is dynamic. Mitigation measures can displace ML to other parts of an economy or drive threats to act in different ways. The process of an NRA is an ongoing process. It’s important that countries feedback on what went well in the NRA process and take steps to improve future iterations.

This final section identifies three parallel activities that countries should undertake after the finalisation of their ML NRA:

- i. Align AML Strategies and Policies with Risk
- ii. Outreach and Stakeholder Engagement
- iii. Feedback and Improving the NRA Process

#### Align AML Strategies and Policies with Risk

It’s important that the NRA process and its outcomes are useful to inform the country’s AML regime. The conduct of an NRA should not be a bureaucratic process without outcomes. The NRA should serve as a foundational element for the country’s decision makers to align national strategies and policies with its risk environment. This includes, as detailed in INR.1, to “(i) inform potential changes to the country’s AML/CFT regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of AML/CFT resources by competent

authorities”, and “national AML/CFT/CPF policies, informed by the risks identified”, as required in R.2.

An NRA should have tangible impact on a country. Case studies show that a well-positioned and effectively utilised NRA can bring significant benefits to enhance the AML systems of a country. Therefore, countries should not see the NRA as a tick-box exercise. The NRA should be considered a tool to develop understanding of the ML risks in the country and have a positive impact on the country’s AML system at a strategic and operational level.

### **Box 18. Integration of NRA Findings into AML Strategy**

#### **Luxembourg**

The National AML/CFT Strategy is based on the results of the NRA and its periodic updates. The definition and implementation of the National AML/CFT Strategy is ensured by the Interministerial Steering Committee for the fight against ML/FT (the Steering Committee) and the Committee for the Prevention of ML/FT (the Prevention Committee), both supported by a permanent Executive Secretariat

The Steering Committee is comprised of the Ministry of Justice, the Ministry of Finance, the Ministry of Interior Security, and the Ministry of Foreign and European Affairs. These ministries play a vital role in the AML/CFT landscape. The Steering Committee draws up the multiyear National AML/CFT Strategy, presented to the Government Council for adoption. The National AML/CFT strategy sets out the main priorities for combating AML/CFT and defines high-level strategic objectives that are further refined by more operational objectives. The Steering Committee reports to the Government on the progress made in implementing the National AML/CFT strategy.

The Prevention Committee coordinates the implementation of the National AML/CFT strategy through its operational members (representatives of the Ministry of Justice, the Ministry of Finance, supervisory authorities and SRBs, the FIU, the prosecution and investigation authorities and representatives of professional associations). Following the current National AML/CFT strategy, categorised into different priorities, the Prevention Committee counts five working groups, gathering relevant representatives from the Prevention Committee and supported by permanent resources from the Executive Secretariat: Risk and statistics (responsible of conducting the NRA process), Supervision, Preventive measures, Transparency of legal persons and legal arrangements, and Detection, investigation and prosecution.

Critically, aligning AML strategies with risk should not solely be seen as a requirement to apply enhance mitigation measures to higher risk situation. Aligning AML strategies with risk means also means that lower risk areas should be subjected to simplified or lesser measures.

#### ***Development of an Action Plan***

Developing an action plan based on the NRA findings can aid the country develop tangible, risk-based mitigation measures for identified risks. Countries should prioritise risk-mitigating strategies based on objective criteria to strengthen their AML system.

Any eventual action plan resulting from the NRA can be adopted at the appropriate government level and supported by the necessary resources to cover all prioritised risk mitigation measures

[see box 19]. It should include actions to reduce the ML risks. These items should be specific and actionable, considering the needs and capacity of stakeholders, bearing in mind any resource constraints. They should be prioritised using a risk-based approach. Involving all relevant stakeholders throughout the process and developing ongoing mechanisms for communication and coordination can facilitate the agreement of recommended actions by ensuring buy-in early, encourage continuous collaboration and guarantee that stakeholders feel ownership and responsibility for the action plan. Countries can also identify key performance indicators (KPIs), to monitor and measure the implementation of actions.

### **Box 19. Action Plans Based on the NRA Findings**

#### **Kingdom of Saudi Arabia**

Following the adoption of the ML/TF NRA Saudi Arabia adopted a national strategy for AML/CFT, and an associated National Action Plan. The national strategy sets out high-level strategic objectives to improve the Kingdom's effectiveness in different areas of AML/CFT policy and operations. The prioritised recommended actions are based on the findings of the NRA related to vulnerabilities and the corresponding risk ratings. The action plan sets out more specific actions, with corresponding indicators and timetables and reflects the specific findings of the NRA. As a result of the action plan, Saudi Arabia released circulars and guidance to supervisory authorities and private sector, and updated exiting laws in line with the risks identified. The Anti-Money Laundering Permanent Committee (AMLPC) was responsible for preparing the NRA, and also for monitoring implementation of the action plan.

#### **Nigeria**

Nigeria's Strategic Implementation Roadmap (SIR) serves as its AML/CFT action plan in line with the country's National AML/CFT/CPF Strategy. It captures all the recommended actions from Nigeria's NRA, and items have been prioritised based on risk. Nigeria has made efforts to foster national cooperation and align the implementation of the action plan with other national strategies on terrorism financing, anti-corruption and drug control, by introducing quarterly meetings between the units responsible to share information and data, organise joint events and facilitate the exchange of expertise to promote joint objectives. An MOU has been signed by the FIU (as Secretariat of the Inter-Ministerial Committee on AML/CFT/CPF) and the Technical Unit on Governance and Anti-Corruption Reforms as well as the Secretariat of the National Drug Control Master Plan to formalise the procedures that will ensure proper alignment of the strategies in practice. The Technical Assistance Subcommittee of the IMC (part of the FIU), is responsible for monitoring the implementation of the SIR and presenting annual performance reports at the IMC's annual review meeting.

A country has the flexibility to determine how it will ensure that national strategies and activities are risk-based. Some options include the following:

- Amending or developing legislation and regulation;
- Developing and/or improving national and international cooperation mechanisms;
- Expending resources, budget and conducting capacity building;
- Risk-based supervisory actions;
- Investigations, prosecutions and asset recovery.

#### ***Amending or Developing Legislation and Regulation***

The NRA will often show gaps or weaknesses in its AML framework that could be exploited by criminals. One common outcome of the NRA can involve changes to the legislative or regulatory framework of the country to fill these gaps. For example, the scope of the DNFBPs can be expanded, as necessary, based on the results of the risk assessment.

This process takes time and involves multiple stakeholders, including policy makers, legal experts and relevant government agencies to ensure that the proposed laws are comprehensive and effective, and align with international standards and good practices. Early and ongoing consultations with non-governmental stakeholders such as the private sector and civil society are also recommended to address any concerns early and avoid unintended consequences once the laws are enacted. An analysis of the effectiveness of these laws should be considered in the next version of the NRA to ensure the law is having the planned impact, and so that the country can amend it further if needed.

### Box 20. Risk Mitigating Measures in Response to NRA Findings

#### France

As a result of the NRA, France introduced several measures to limit anonymity in sensitive sectors such as funds transfers and money exchange. France limited the use of cash and transactions carried out using pre-paid cards to mitigate some of the most important typologies identified.

France also extended AML/CFT obligations to certain financial and non-financial sectors beyond the scope of the FATF requirements in order to mitigate some major risks. For example, France introduced the requirement for supervision of the handling of funds channelled through self-regulated professions. judicial trustees and notaries are required to operate in conjunction with the Deposit and Consignment Office (CDC) and lawyers with the management fund for lawyers' fees (CARPA) when handling funds. The inclusion of CARPAs in the AML/CFT regime in 2020 allowed France to strengthen measures to identify and mitigate the most important risks for the profession.

#### Korea

Korea has made several legislative changes in line with the findings of its NRAs. Following its 2018 NRA, which identified the abuse of VA as a high-risk vulnerability due to the anonymity permitted in transactions, it brought VASPs within the scope of the AML/CFT framework and imposed enhanced consumer protections and limitations on use of VA.

The abuse of cash was also noted as a high-risk vulnerability in the NRA due to the anonymity and a review of ML case studies that showed that cash is the most common ML instrument. To address this, Korea lowered the threshold for cash transaction reports. It also aimed to improve CTR reporting.

### Developing and/or Improving National and International Cooperation Mechanisms

The NRA process brings together a range of national authorities across operational, policy and supervisory functions, and in many cases involves elements of international cooperation with neighbouring countries, international organisations and IFIs. It also involves various non-governmental stakeholders that can be greatly impacted by the NRA results. The NRA exercise itself may help to discover some coordination and information sharing challenges and improve national coordination.

On a domestic level, the NRA can provide platforms and fora for exchange of ideas and information which should be encouraged on an ongoing basis as it breaks down silos between different agencies, promotes a shared understanding of ML risk and demonstrates that the NRA is a continuous process. Some countries develop Public-Private Partnerships (PPPs) that continue after the NRA, allowing for ongoing discussions on risk with those on the front lines. Maintaining these relationships and facilitating ongoing communication builds trust among stakeholders and promotes a more holistic approach to risk. It also allows for more efficient follow up and monitoring on risk mitigation measures and their efficacy. It is recommended to make every effort to ensure that the high level of coordination and cooperation observed during the NRA is maintained after its completion.

### Box 21. National Coordination

#### Norway

Norway introduced a national coordination mechanism called The Contact Forum in 2015 to coordinate actions to assess risks. It includes a wide range of stakeholders within the AML/CFT regime. The Contact Forum is specifically mandated to identify ML/TF threats and trends, coordinate work to develop AML/CFT strategies and oversee development of Norway's NRAs. Coordination and cooperation among national authorities has improved significantly since the establishment of this forum and help facilitate information exchange and provides updates on policy work at a domestic and international level.

Concerning operational authorities, the LEA's national IT system called Indica facilitates coordination, cooperation and information sharing between the FIU and LEAs. LEAs including police districts, include their investigation information into the system, and the FIU can access this information and add its own information into the system because the FIU system is connected to Indicia, facilitating the sharing of investigative information and financial intelligence.

### Box 22. International Cooperation Good Practices

#### United Kingdom

LEA policies respond to the ML risks identified in the NRA. International liaison officers are posted abroad to higher-risk countries to enhance the UK's ability to obtain and provide international co-operation. LEAs have coordinated projects to raise intelligence and improve understanding in high-risk areas, including on high-end ML, cash-based ML, ML through professional enablers, and organised crime. The UK collects a range of qualitative and quantitative information which feed into its risk understanding and is used in policy development. This could be supplemented by consistent, comprehensive, national statistics on all ML investigations, prosecutions, and convictions; confiscation; and international cooperation.

LEAs are also making progress on developing policies to address emerging risks, such as cash in freight.

#### ***Expending Resources, Budget and Conducting Capacity Building***

The NRA can highlight gaps in resources, capacity and expertise at all levels of a country's AML system and inform important decisions on prioritisation and reallocation of resources.

Based on NRA findings, policymakers and regulators can allocate resources more effectively to address identified gaps and enhance the country's AML capabilities. Budget and resources may be reallocated to higher risk areas, e.g., increasing funding for certain LEAs and improving investigations in line with the highest risk predicate offences, or to supervisory authorities to enhance their capacity for conducting on-site inspections in particular sectors. A risk-based approach involves directing resources away from areas identified in the NRA as lower-risk, and

towards higher-risk areas, and can help countries with less mature NRA processes manage their resources more effectively. The NRA could also prompt the recruitment of specialised personnel, such as financial investigators, intelligence analysts, and legal experts, to bolster the country's capacity to detect, investigate, and prosecute financial crime effectively.

Increasing the number of staff in high-risk areas can be a good first step, but more importantly countries should ensure that all staff operating in the AML system have the capacity and knowledge to do their jobs effectively. By identifying areas where training is lacking or outdated, the NRA can inform the development of training programs tailored to the specific needs of all stakeholders involved in AML efforts. These training programmes can cover a range of topics, including risk assessment methodologies, financial investigation techniques, regulatory compliance requirements, and emerging trends in financial crime. Through investing in capacity building and training, a country can enhance the competence and professionalism of their AML personnel, thereby improving the effectiveness of their efforts to combat financial crime.

The NRA may also demonstrate areas that can be made more efficient. Automating or digitising certain manual processes and introducing or adapting IT tools can save time and resources at both national and organisational levels, allowing experts to focus on the substance of their work.

### Box 23. Training and Capacity Building

#### Brazil

Brazil has developed actions and policies to address the threat of corruption and associated money laundering from various initiatives. One such initiative is the creation of the National Training Program to Combat Corruption and Money Laundering (PNLD), which provides training for government officials and allows them to share knowledge about their efforts on these issues. In addition, Brazil established the National Network of Anti-ML Technology Laboratories, which provides a network for sharing expertise and experiences in detecting ML, corruption and other crimes related to large-scale data analysis. These steps, combined have served to upskill Brazil's staff in combating corruption, and the laundering of the proceeds of corruption.

### *Risk-based Supervisory Actions*

The FATF Standards require supervision to be proportionate to the risks arising from different FIs, VASPs and DNFBPs. The findings resulting from the NRA play a fundamental role in shaping prioritised supervisory actions, such as the allocation of resources to supervise sectors on a risk-basis. The FATF issued guidance on risk-based supervision in 2021<sup>11</sup>, outlining how supervisors can prioritise their activities in line with risk.

Risk understanding is a two-way process - The NRA relies on supervisors' understanding of sectoral risks, and supervisors develop an updated understanding of threats to their sector from predicate crimes, typologies, and ML/TF threats through involvement in the NRA process. Supervisors should consider whether the conclusions of the NRA on a sector-basis are coherent with their understanding of the aggregate entity-level risk ratings they have developed. This analysis should

<sup>11</sup>. [www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-supervision.html](http://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-supervision.html)

influence supervisors' actions in areas such as the type and intensity of licensing controls, the frequency and intensity of on-site and off-site supervision, guidance provided to covered sectors and other risk-mitigation strategies.

### **Box 24. Risk-based Supervision**

#### **Bermuda**

The BMA has put in place a risk-based ML/TF supervisory framework to assess compliance with FIs and TCSPs under its supervision and to mitigate sectoral risks. This framework assesses the impact and probability of risks with respect to all aspects of the institutional FIs' operations and controls on an ongoing basis in order to facilitate a timely supervisory response to identified weaknesses or possible failures. Sectors considered high risk (banks/credit union, securities sector, private trustees and corporate service providers) are prioritised for supervision by the BMA and all supervised entities are subject to onsite examinations and offsite monitoring. Onsite Examinations are decided upon at the beginning of the year and the calendar of inspections can be revised during the year based on changes in the risk profile of institutions, including factors and the results of "refresh" risk assessments.

The NRA provides good opportunities for coordinated regulatory response, particularly for high-risk sectors. For example, in a country where the real estate sector poses higher ML risks, supervisors of real estate agents, lawyers, financial institutions providing housing loans and mortgage services, and TCSPs can coordinate their regulatory response to address the heightened risks. Supervisors should collect data on key performance indicators to demonstrate the impact of their supervision.

#### ***Investigations, Prosecutions and Asset Recovery***

The NRA should have an impact on shaping the RBA to the investigation and prosecution of money laundering and the associated asset recovery. As mentioned throughout the report, LEAs should actively contribute to the NRA process by providing data and qualitative insights and take ownership of its findings. Measures that are introduced should enable LEAs to focus on pursuing investigations, prosecutions and asset recovery in line with the identified risks. Encouraging LEAs to focus their resources on the highest risk predicate offences or types of ML that take place in the country can lead to the successful conclusion of more impactful ML cases.

LEAs can also gain useful information from the typologies and methods that are elaborated in the NRA and can adjust their intelligence and investigation techniques and strategies to target key risk factors to bring about more effective results. This can include the creation of specialised task forces or departments to tackle particular crimes. LEAs can also develop reports on typologies or themes to refine their own understanding of risks.

The NRA also strengthens collaboration and information sharing between LEAs, FIUs and regulatory agencies, among other stakeholders. This can help initiate joint investigations and maximise the impact of supervisory actions.



### **Box 25. Measures to Improve Investigations and Prosecutions in line with Risk.**

#### **Netherlands**

The Netherlands proactively initiates ML investigations through police intelligence signals detected in the course of investigations into predicate offences, as well as through financial intelligence developed by the FIU-NL. In addition, the authorities adopted an innovative approach by launching thematic AML projects based on the ML risks in the NRAs to increase their ability to detect new ML schemes and typologies, resulting in additional cases identified. Dutch authorities pursue a wide range of investigations, from self-laundering to complex cases, including offshore companies, professional money launderers and VAs. Based on the NRA findings, they also have dedicated resources to countering organised crime groups which are in line with their risks identified.

#### ***Response to Lower Risks Areas and Promotion of Financial Inclusion***

Within the framework of AML efforts, identifying and categorising lower-risk areas is essential for efficiently allocating resources and directing attention towards sectors with higher inherent risks. The FATF Standards permit countries to take simplified due diligence (SDD) measures to manage and mitigate risks, where lower risk areas have been proven and there is no suspicion of ML/TF activity. The outcomes of the NRA provide an ability for countries to implement these SDD measures. Countries should ensure that vulnerabilities are adequately identified and managed, thereby upholding the integrity of the overarching AML framework. Lower risk areas should be carefully monitored for any change in circumstances that may raise the risk level. Practically, lower risk area is determined by proven low ratings in terms of threat, vulnerability, and consequence (if the country assesses so).

An effective approach to SDD requires countries, FIs, DNFBBs and VASPs to develop a comprehensive understanding of the contextual factors impacting the ML/TF risks in the country. This can be provided by the NRA. This country-level risk assessment should identify higher and lower risks and allow for the identification by institutions of lower-risk situations where simplified measures can be implemented. The criteria for designating an area as low risk encompass several key factors. The regulatory framework must be robust and transparent, including clear and comprehensive AML regulations. Additionally, there must be effective oversight and enforcement by competent authorities, with regular inspections, audits, and assessments ensuring compliance with AML regulations and identifying any potential weaknesses or gaps in existing controls. Historical data can also indicate minimal levels of illicit financial activities with comprehensive statistical and trend analyses of previous years' STRs and other relevant data providing valuable insights into the prevalence and nature of money laundering activities in specific areas.

Assessments and identification of lower-risk areas should be documented and regularly updated, with the purpose that supervisors can identify the appropriate determination of risks and situations where the use of simplified measures by financial institutions may be appropriate.

Increasing the granularity and level of detail of risk assessments can be an avenue to improve risk understanding, thereby supporting the promotion of financial inclusion. Frequently, different entities within the same sector are exposed to a different level of risk, or a different kind of risk, by virtue of their different activities or different customer groups. A risk assessment that aggregates such different entities and customer groups may assess the risks incorrectly and result in

inappropriate level of risk mitigation measures being applied by regulators and regulated entities. Disaggregating such entities and customer groups and setting out how the risk profile of each group is rooted in their activities and customer bases, can enable a more fine-grained approach to risk management by financial institutions and competent authorities. For example, this can include applying different controls to the highest-risk or lowest-risk entities and customer groups within a particular sector, rather than a single level of control for the entire sector; or it can enable one kind of risk mitigation measure to be substituted for another, less obstructive measure.

Countries should exercise caution and differentiate between a proven absence of risk-aggravating factors, and a lack of relevant statistics, which can lead to a misconception of low risk. The FATF Standards allow exemptions from certain recommendations to be applied to proven lower risk areas in certain circumstances. Therefore, countries must understand the consequences of concluding that an area is lower risk, as it may have substantial implications for the effectiveness of AML protection in that particular area.

### **Box 26. Challenges and Solutions in Identifying Lower Risk Areas**

#### **New Zealand**

New Zealand has faced challenges in defining and managing lower risk areas, particularly where ML activity is infrequent. Establishing the absence of risk can be challenging, as the lack of evidence does not necessarily equate to low risk. To address these challenges, New Zealand emphasises the use of robust risk assessment methodologies to more confidently identify and manage areas of low risk. Clear guidance is crucial, emphasizing comprehensive methodologies that differentiate between "real," "possible," and "theoretical" risks. New Zealand highlights the importance of delineating risks in national discourse to ensure a nuanced approach.

New Zealand recognises the risk of confirmation bias and advocates for a broader view in the identification phase, drawing from various sources such as case data, intercept transcripts, and interviews with criminals. Leveraging intelligence from diverse sources, including overseas, enhances New Zealand's understanding of unknown threats.

Adherence to best practices, like ISO 31000, strengthens New Zealand's risk assessment methodologies. Integrating insights from domestic and international sources ensures a comprehensive approach to managing money laundering risks, even in areas considered low risk due to limited domestic data.

Limited exemptions in areas with proven low risk is an option for countries and should not be dismissed. Calibrated and well-justified exemptions in lower risk areas can allow more strategic reallocation of some resources and improve the overall effectiveness of AML system and improve financial inclusion.

## Box 27. Financial Inclusion

### India

India has taken several steps to promote financial inclusion with the aim to maintain financial integrity, by designing financial inclusion products with in-built risk mitigating measures. A sectoral risk assessment concluded that the overall vulnerability of these financial products is low as far as they relate to ML/TF therefore India has put in place simplified measures to allow broader access to the formal financial system.

To help ensure that people with lower incomes in India have access to banking, the Prevention of Money Laundering Act (PMLA) allows for simplified CDD in the opening of “small accounts” as defined in its rules, as well as other accounts for categories of clients that are low risk. The rules do not permit simplified measures where there is a suspicion of ML/TF, where specific higher-risk scenarios apply or where the risk identified is not consistent with the national risk assessment.

Significant transactions in the informal economy in India happen in cash. Based on India's assessment of the risks associated with cash, India introduced policies (known as Jan Dhan, Aadhaar and Mobile) to encourage use of the formal financial system. These policies expanded affordable access to bank accounts and other financial services, using a biometric identification system and supported the development of a digital mobile payment system.

India has prioritised the development of digital payment infrastructure, leading to a rapid increase in digital transaction volumes from 20.7 billion transactions in 2017-18 to 134.6 billion in 2022-23.

As a result of these measures, access to financial services has increased from 35% of the total population in 2011 to 80% in 2017.

### Philippines

In the Philippines second NRA, financial inclusion products were rated as lower risk, due to the small amounts of funds involved and the low threshold amounts of products, and also due to the limited functionalities of the products and small target market (the underserved local population). The Philippines mainly used data from the supervised financial institutions of the Bangko Sentral ng Pilipinas to develop the risk analysis, which is systematically collected on an ongoing basis to ensure an up-to-date risk understanding, including to inform the Philippines third NRA which is in process.

The results of the second NRA supported the Bangko Sentral ng Pilipinas' current ambitious financial inclusion strategy. The level of formalisation of the economy has improved to medium from medium-low since the second NRA, due to the government's financial inclusion initiatives which target the needs of the unbanked and underserved population.

For more information on SDD measures and other measures to support financial inclusion, please refer to the separate FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion.<sup>12</sup>

## Outreach and Stakeholder Engagement

Countries should proactively communicate the findings of the NRA, including any updates thereof, during the interim periods between formal publications of the NRA. This chapter proposes a strategic approach to enhance communication and overcome the challenges associated with this process, which can be summarised as follows considering experiences from the Global Network:

- **Continuous** – Countries should adopt a continuous approach to the communication plan and outreach of the NRA findings to stakeholders, so the needs and expectations of the target audience(s) are considered throughout the NRA process. Continuous communication of the NRA findings enhances stakeholders' risk awareness and understanding. It develops a sense of accountability among stakeholders for the implementation of risk-mitigating measures. Countries can also use the communication of the NRA findings to promote information sharing among stakeholders, including workshops and forums for sharing best practices and challenges faced. Continuous communication also helps governments obtain up to date information on emerging risks and challenges which can support policy making and allow them to be more proactive. Other publications, such as typologies and red-flag indicators should also be used for more agile communication of risk updates and emerging/new risks.
- **Differentiated** – A distinction may be made between public and non-public communication. This may involve the use of different media platforms such as social networks, commercial publications, presentations etc. aimed at different stakeholders. Some countries publish different versions of NRAs, such as a restricted version for government agencies' consumption, a public version and even sector specific versions - this has been reflected by the private sector as a good practice to enhance their understanding of the NRA findings, while preventing the compromise of sensitive information. Outreach to ensure understanding of risk should be similarly differentiated to focus on the details relevant to each stakeholder/sector.
- **Transparent** – Countries can share the NRA publicly for transparency, to support decision making, public participation, stakeholder engagement and private sector/civil society feedback. Sharing the findings of the NRA alone is not sufficient as it lacks enough context to be useful to stakeholders in developing risk understanding. In this regard, sharing some insights from the methodology aid supervisors and private sector better comprehend the risks and in conducting their own risk assessments. There may be some aspects of the NRA that a country does not want to make available publicly, e.g., confidential intelligence sources, national security concerns and the potential economic impact of risks materialising. Countries are recommended to disseminate restricted information through secure platforms such as GoAML or by supervisors to their respective sectors. For example, the British Virgin Islands produced a sanitised version of its NRA with sensitive law enforcement information removed, which is published for public consumption, whereas a full version is made available to relevant competent authorities.

- **Risk-based** – Countries may consider a phased approach to outreach, targeting the higher-risk stakeholders first in line with the risk-based approach. This communication and outreach may be more detailed and bespoke, and held in person, with more discussion, consultations and follow-up activities with the higher-risk sectors to ensure they have a comprehensive risk understanding. Supervisors that supervise multiple entities should also take a risk-based approach to communications. To enhance understanding of the NRA findings, countries relied on a variety of actions:
  - **Inclusion in Process** - it is vital to include stakeholders, including the private sector, in the early discussions, planning and drafting phases of the process and ensure outreach planned corresponds to their needs.
  - **Publication of NRA** – as mentioned above, countries frequently produced a public version of the NRA, and an adapted version for reporting entities which is more targeted to their needs. Several methods were cited to publicise the document, e.g., use of social media, development of information videos, distribution on the websites of competent authorities, circulating via mailing lists to stakeholders as is done for other significant publications. Furthermore, countries could consider translating the NRA to enhance understanding in countries with more than one official language and to make it more accessible to other countries. Updates and refinements in red-flag indicators based on the NRA can also be very useful for the reporting entities.
  - **Targeted Training/Workshops** – A good practice highlighted by several countries is to organise sector-specific workshops, presentations or webinars to target the content appropriately to each sector. This can also lead to more constructive feedback through question-and-answer sessions. Some countries also provide an online training package for ease of stakeholders’ access to relevant information. Whilst options such as a webinar can connect to a broader audience, many countries recognise the power of in-person engagement. A balance between the purposes, resources and intended outcome should be struck when considering the optimal outreaching method.
  - **Linking NRA to Supervisory Activity** – some countries suggested incorporating the NRA into on-site inspections to encourage an up to date understanding of risk among reporting entities, and to ensure the findings of the NRA have been incorporated into industry level risk assessments. The lead agency of the NRA can also have regular meetings with reporting entities to raise awareness of the NRA findings and receive feedback. It is important to emphasise the practical implications of the NRA findings on the risk-based approach that supervisors must apply in the conduct of their supervisory activities and that the private sector must apply in conducting their day-to-day business.

Based on feedback received during the outreach phase of the NRA, some countries introduced further initiatives to support risk understanding among the private sector. Some examples shared by countries of methods for engaging with stakeholders on the NRA findings and risk in general are below.

## Box 28. Stakeholder Engagement on Risk

### Canada

The Government of Canada, through the Department of Finance, publishes a public-facing report of the inherent money laundering and terrorist financing risks. This report provides critical risk information to the public and, in particular, to the regulated entities across the country that have reporting obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, whose understanding of inherent, foundational money laundering and terrorist financing risks is vital in applying the preventive measures and controls required to effectively mitigate these risks. This report specifically examines these risks in relation to key economic sectors and financial products in Canada and it assesses the extent to which features make Canada vulnerable to being exploited by threat actors to launder funds and to finance terrorism. It is meant to raise awareness about Canada's risk context and the intrinsic properties that expose these sectors and products to money laundering and terrorist financing risks in Canada. The vast majority of businesses, professions and sectors assessed in this report follow Canadian laws and contribute to the social and economic prosperity of the country; only a very small subset of actors are complicit in illicit activities such as money laundering. In March 2023, the most recent version of the report was published at [www.canada.ca/en/department-finance/programs/financial-sector-policy/updated-assessment-inherent-risks-money-laundering-terrorist-financing-canada.html](http://www.canada.ca/en/department-finance/programs/financial-sector-policy/updated-assessment-inherent-risks-money-laundering-terrorist-financing-canada.html).

FINTRAC, Canada's FIU, has led the social media efforts to communicate the national risk assessment on both X (formerly Twitter) and LinkedIn. The Department of Finance Canada has been actively presenting the report to interested private sector organizations, leveraging established connections through the Advisory Committee on Money Laundering and Terrorist Financing, the Canada Revenue Agency's Not-For-Profit Advisory group, and the Counter Illicit Finance Alliance of British Columbia (CIFA-BC). The Department of Finance is working to communicate the findings of the 2023 report to private sector members via sessions tailored to each sector. The NIRA report is included in various other stakeholder engagements, as are other documents providing an assessment of risks.

### Democratic Republic of Congo

The Democratic Republic of Congo conducted a vast campaign to disseminate the findings of its 2023 NRA to stakeholders across its vast geographical area and 26 administrative provinces. The findings were shared to all competent authorities in the months following the NRA's finalisation and approval by the Council of Ministers through official letters. The country also hosted 28 awareness raising sessions for competent authorities, FIs and DNFBPs across the country to ensure understanding among all stakeholders.

## Feedback and Improving the NRA Process

The ML NRA process itself can be influenced and improved based on the findings and lessons learned from each iteration of the assessment. Countries are encouraged to review their NRA process on a regular basis and make changes to improve its effectiveness.

Countries may make changes to certain aspects of the governance of the process, for example refining the methodology and mechanisms to make them more appropriate for the country's situation. As many countries encountered issues obtaining accurate and complete data sets during their first NRA, some decided to invest in data collection and analytical tools or introduce standardised forms. They may also introduce new information-sharing mechanisms and aim to change the data collection and sharing culture among agencies. Countries should assess the various stages of the NRA timeline and aim to streamline where possible, including eliminating redundancies, finding efficiencies in stakeholder engagement and improving workflows.

One factor to analyse is whether risk-mitigation measures introduced following the previous NRA are having the desired effect. With the best intentions, some risk-mitigation measures may lead to unintended consequences. These could be related to various topics, for example overly restrictive measures may lead to an adverse impact on financial inclusion and prohibit marginalised communities from accessing financial services. Countries must be aware of the possibility that increases in regulation may result in some businesses using a "tick-box" approach to meeting regulatory requirements rather than an RBA. This can lead to inadequate risk-management efforts and steps should be taken to avoid this. Implementing risk mitigation measures in one area may displace the risks to another sector or type of transaction, e.g., increased due diligence in traditional financial institutions may lead to criminals exploiting sectors with less stringent regulation like virtual assets. This highlights the importance of viewing the NRA as a process – countries should constantly evaluate the actions they are taking and be able to adjust them when needed.

Many countries that responded to the questionnaires actively seek feedback from stakeholders including the private sector on ways in which they can improve their process. This can be done in different ways, both formal and informal, for example through surveys, targeted questionnaires, roundtables or focus groups. The public consultation for this project showed that according to the private sector, roundtables and surveys are among the most effective ways for them to provide feedback on the process. Many encouraged the use of online tools to facilitate this, including email correspondence, dedicated websites and web applications. They also encouraged countries to leverage private sector expertise through expert panels, advisory boards or public-private partnerships to offer recommendations. Another strong theme in responses was that it is more efficient for the private sector to be involved in the NRA process throughout and provide ongoing feedback so drafts can be adjusted accordingly before the product is completed.

Outreach to stakeholders on the findings of the NRA can also be useful for gathering feedback on how the NRA process could be more useful to them and how the findings and other information on risk could be better communicated. It is highly recommended that countries consult with all stakeholders to continuously develop and improve their process to make it more effective. Some examples of information that has been requested from the private sector to help develop their risk understanding are:

- i. Risk indicators on common predicate offences.
- ii. Statistics related to predicate offences and ML.
- iii. Case studies demonstrating the risks identified.
- iv. Guidance on how to implement the findings of the NRA.

Countries could also introduce key performance indicators (KPIs) to show the impact of the NRA. According to the responses received to the questionnaire, most countries do not have an established approach to collecting and analysing KPIs. Some countries have introduced analytic technologies to the website where the NRA is published that assess the frequency of the NRA being accessed or cited. Countries could also consider looking at other objective data points to see what impact the NRA has had on different aspects of the AML system, for example:

- **Risk mitigation measures implemented** – countries should monitor the implementation of the action plan resulting from the NRA and report back on progress and any challenges encountered. Countries could track how many actions have been successfully launched or completed, whether they are taking place in the expected timelines etc. This can help a country produce more accurate and feasible actions plans for future iterations of the NRA.
- **Improved Collaboration** – The NRA should improve cooperation on a national and international level. Countries can evaluate the performance in areas such as establishment of communication and coordination channels in domestic and international levels, level of participation, and tangible work product, etc.
- **Effectiveness of Supervisory Activity** – Countries can assess FI and DNFBP compliance with AML regulations and track progress and improvements based on the measures implemented. This may include the results of supervisory inspections, the frequency of inspections in line with risk, and the application of proportionate and dissuasive sanctions for non-compliance.
- **Increase in STRs Filed** - The highest risk sectors should be encouraged to file STRs. Depending on the maturity of the sector, training and outreach may be needed to ensure STRs filed are good quality.
- **Increase in Investigations and Prosecutions** – As mentioned earlier in the chapter, countries should see an increase in investigations and prosecutions in line with the highest risk areas. This data can be used to demonstrate the operational impact of the NRA on the activities of LEAs.
- **Effectiveness of Training and Capacity Building** – Many countries reallocate resources and develop training in response to the NRA findings. Some countries test the effectiveness of this by incorporating tests on risk into supervisory activities to ensure understanding of the NRA findings. Other data points could include number of people trained and from which agencies, feedback from trainees, results of tests or exercises completed as part of the training.



## Section Conclusion

**Table 5. Section 3 Key Points**

This table highlights the key elements of steps to take after the completion of the NRA.

Sub-section	Key points
Align AML Strategies and Policies with Risk	<p>Ensure the <b>national strategies and policies are responsive to the findings of the NRA</b>.</p> <p>Develop <b>risk-responsive action plans</b> and prioritise implementation of action items on the basis of risk. Identify timelines, assign responsibilities, and have a mechanism for ensuring accountability and timely delivery of actions.</p> <p><b>Lower risk areas should receive consideration for simplified or less intense risk mitigation measures.</b></p> <p><b>Reallocate resources from lower risk areas to higher-risk areas</b> based on the NRA findings and aim to further build capacity of the authorities through training.</p>
Outreach and Stakeholder Engagement	<p><b>Communicate findings to all relevant stakeholders</b> from competent authorities and private sector.</p> <p>Take a <b>targeted, risk-based approach to following up with stakeholders</b>. Level and content of engagement should be tailored to risk and needs of stakeholders.</p> <p>Aim for a <b>continuing discussion on risk between stakeholders</b> to form the basis of the NRA as an ongoing process.</p>
Feedback and Improving the NRA Process	<p><b>Review the NRA process and modify it</b> based on lessons learned to improve future iterations.</p> <p><b>Seek feedback from stakeholders including the private sector</b> on how they use the NRA findings and how the process (to include any resulting document) could be more useful for them.</p>

## Annex A. Types of Risk Assessments that Complement the NRA

This annex complements the information in section 3.3.3 which discusses the different types of risk assessment and how they can link to the NRA and enhanced a country’s risk understanding.

### Sectoral and Thematic Risk Assessments

Sectoral and thematic risk assessments allow countries to focus on emerging sectors or areas of increasing risk without having to wait for or carry out an update of the NRA when it would not be practical or efficient to do so. They also enable countries to develop a more detailed understanding of the threats and vulnerabilities and the existing mitigating measures in relation to a specific area of interest, for instance in relation to a material sector or a predominant threat. The results of sectoral and thematic risk assessments complement those of the NRA and can likewise be used to coordinate the actions of authorities and inform the private sector. The results may also be taken into consideration for the purposes of subsequent updates of the NRA.

Advantages	Potential Shortcomings
<p>Deep dive – Narrowing the scope of a risk assessment to a specific sector allows for the development of typologies on how the sector may be abused for ML purposes and by whom. It allows authorities a deeper understanding of industry-specific vulnerabilities and mitigating measures that are in place.</p> <p>It can be an effective way of examining new/emerging sectors in detail, or sectors where the risks have changed due to emerging threats or changes in legislation and regulation. The NRA methodology may be adapted to the sectoral/thematic assessment.</p> <p>E.g., Australia developed a risk assessment on remittance corridors between Australia and the Pacific Islands with the goal of providing more information on the ML/TF risks associated with remittances sent through remittance providers from Australia to Pacific Island countries and assist remittance providers and banks to identify lower-risk transaction types and scenarios.<sup>13</sup></p>	<p>Limited scope - Isolated Sectoral risk assessments may have a narrow focus and ignore cross-cutting issues that impact multiple sectors (e.g., use of cash). Although broader than a sectoral risk assessment, a thematic risk assessment may lack analysis on broader systemic issues and interconnections between different typologies and sectors. This may lead to gaps in risk identification and mitigation.</p>
<p>Agility - Thematic and sectoral risk assessments can be more flexible and adaptable than broad national-level assessments, allowing for quicker responses to emerging threats, changes in regulations, or shifts in industry practices.</p>	<p>Data challenges – Countries may encounter challenges when assessing certain sectors or themes (e.g., emerging sectors, unsupervised sectors or those that have recently been brought under regulatory frameworks). In these cases, countries may rely on academic reports and open-source intelligence to develop the risk assessment, but it may limit the accuracy of the findings and conclusions.</p>
<p>Targeted risk mitigation measures - Sectoral risk assessments facilitate the development of targeted risk mitigation measures and regulatory interventions that are tailored to the specific needs and characteristics of the industry.</p>	<p>Fragmented approach – Addressing the risks of only one sector or theme may lead to a country attempting to address its risks in isolation without considering broader consequences across the AML system.</p>
<p>Industry collaboration – This approach encourages collaboration and information sharing practices among governmental authorities, industry participants, supervisory authorities, specialised experts and</p>	<p>Lacks holistic view – These approaches may not be able to consider factors such as macroeconomic trends, geopolitical events or other changes in legislation or regulation that may</p>

<sup>13</sup> [reference: [remittance-corridors-risk-assessment.pdf \(austrac.gov.au\)](https://www.austrac.gov.au/remittance-corridors-risk-assessment.pdf)]

other stakeholders. Countries should aim to foster a culture of continuous information sharing and cooperation between stakeholders.	impact multiple sectors/themes. Also, without the input from LEAs, prosecution etc. supervisors cannot have an accurate picture of national crime context and environment.
<p>Reviewing existing measures – Both approaches allow country to explore the impact of existing legislation, regulations, supervisory activity and other risk mitigation measures on the sector or theme.</p> <p>e.g., Denmark has developed several thematic risk assessments on areas such as trade-based ML because of the high risks and there is a lack of understanding of the ML risks associated with it, and use of cash in the criminal economy, as they introduced new legislation to combat it and the vulnerabilities associated with it had changed.</p>	

Note: These potential shortcomings are relevant particularly when sectoral or thematic risk assessments are done in isolation.

The purpose of a sectoral risk assessment is to provide a targeted analysis of money laundering risks within a specific sector, sub-sector, or industry. It examines the unique characteristics, vulnerabilities and typologies associated with the sector, including all activities, services, and products the sector offers, the profiles of customers, business models, how financial transactions occur and any established and emerging trends for usage. It should also look at the sector's exposure to cross-border threats, which could vary depending on the size of the sector, the location of the country and whether clients are citizens of the country or not. Sectoral risk assessments may inform the NRA, but the findings of the NRA may also show a lack of understanding in certain sectors that the country could then prioritise for a sectoral risk assessment after the adoption of the NRA.

Thematic risk assessments focus on specific themes or cross-cutting issues that create ML risks. Countries may choose to focus on an established risk, e.g., use of cash or digital payments that could impact many sectors, or an emerging threat, e.g., cyber enabled fraud, which the country might not have explored in detail and has the potential to become a significant risk. Governments should prioritise themes to explore based on the threat they pose to the country. The thematic risk assessment should aim to understand the risks associated with the selected area of study by analysing vulnerabilities, modus operandi, typologies and potential likelihood and consequences of abuse for ML, including any gaps that may be exploited. Thematic risk assessments generally have a broader reach than a sectoral risk assessment because the themes they deal with can impact multiple sectors or industries.

### Supranational and Subnational Risk Assessments

A supranational risk assessment (SNRA) is analysis conducted at a regional or international level, identifying the ML risks across multiple countries or member states in a regional or international organisation such as the European Union or an FSRB. Normally this will be led by the supranational organisation to ensure that the assessment considers the cross-border threats and vulnerabilities affecting the bloc or region, rather than a consolidation of individual countries' assessments.

Such risk assessments should not replace the national risk assessments to be conducted by the individual member countries, who remain best suited to identify, assess and determine how to mitigate the risks in their own country. The results can however assist individual countries with conducting their own assessments.

Supranational risk assessments allow:

- **Comprehensive Regional Perspective** – Supranational risk assessments provide a comprehensive analysis of risks that transcend national borders, which is particularly important given the cross-border risks related to ML and which cannot always be identified and mitigated through an individual country approach.
- **Standardisation** – This approach may promote the standardisation of risk assessment methodologies, mitigating measures, risk ratings and regulatory frameworks across multiple countries leading to a consistent and collaborative approach to addressing high-risk areas in the region. For example, when conducting their NRA, individual member countries may consider assessing the risks associated with all the relevant products and services assessed under the supranational risk assessment.
- **Information Sharing** – Supranational risk assessments facilitate information sharing and collaboration between countries, agencies within countries and international organisations. It enables and encourages them to share good practices, intelligence and resources to effectively combat ML on a regional level.
- **Enhanced Effectiveness of Risk Assessment** – As supranational risk assessments can utilise the resources and expertise of multiple countries, it enhances the identification and assessment of emerging threats and vulnerabilities and cross-border risks that may not be apparent on a national level.
- **Common Recommendations** - A supranational risk assessment may result in the development of common recommendations for member countries including public authorities and private sector operators, leading to a more robust and harmonized approach towards mitigating the identified risks.

## Box A.1. Supranational Risk Assessments

### European Commission

The European Commission has already published three supranational risk assessments (SNRA), in 2017, 2019 and in 2022. A fourth SNRA will be published in 2025. The 2022 SNRA provides a comprehensive overview of ML/TF risks in the European Union and recommendations for countering them. Article 6(1) of the Anti-Money Laundering Directive requires the EC to update the SNRA in principle every two years, and to reassess all sectors covered in previous iterations and finetunes the information included previously on sectors where the risks have not changed. Where risks have changed, the EC recalculates the risk levels.

The 2022 version analyses current ML/TF risks and assesses how well countries have implemented the previous iterations' recommendations for risk mitigation, evaluating residual risk levels.

The EC did a broad consultation with stakeholders including EU-level organisations, national level experts and academia, as well as considering NRAs of member countries.

Many EU member states reported consulting the SNRA as part of their own NRA process.

Under the new EU AML/CFT framework an AML/CFT risk assessment at Union level (Union RA) will be published in the year 2028 (Article 7 Directive (EU) 2024/1640) and updated every four years. The European Commission may update parts of the report more frequently, if appropriate.

This report shall cover at least the areas and sectors of the internal market that are exposed to money laundering and terrorist financing risks; the nature and level of the risks associated with each area and sector; the most widespread means used to launder illicit proceeds, including, where available, those particularly used in transactions between Member States and third countries; an assessment of the risks of money laundering and terrorist financing associated with legal persons and legal arrangements, including the exposure to risks deriving from foreign legal persons and foreign legal arrangements and the risks of non-implementation and evasion of targeted financial sanctions.

According to the new EU AML/CFT framework there is also a four-year update requirement for NRAs ("at least every 4 years ", Article 8(1) Directive (EU) 2024/1640).

### Eurasian Group on Combatting ML and TF (EAG)

In 2020-2022, the EAG conducted a risk assessment of ML/TF in the Eurasian region, identifying both regional risks, threats and vulnerabilities and sub-regional risks (for specific groups of Member States or supranational entities). Based on the results of the assessment, an Action Plan (Roadmap) to mitigate the identified risks was developed, which includes organisational measures, as well as specific supranational measures aimed at minimising risks, threats and vulnerabilities, including through the formation of regional mechanisms and tools to address technical compliance deficiencies in national legislation and to improve the effectiveness of national AML/CFT/CPF systems.

EAG members are encouraged to use the results of this supranational risk assessment to inform their NRAs, and many EAG members reported consulting it as part of their national level risk assessment process.

A sub-national risk assessment looks at ML risks specific to a particular geographic area and is commonly used by countries with a federal system or a large geographic reach including overseas territories. If a country undertakes multiple sub-national risk assessments, it should also consider consolidating these findings in an NRA.

Sub-national risk assessments allow:

- **Granular Understanding** - Sub-national ML risk assessments provide a granular understanding of ML threats and vulnerabilities within specific geographic areas, such as cities, regions, or districts. It considers factors that make it different to other parts of the country, e.g., the demographics that live there, the proximity to a border, economic development, levels of crime, which allows for targeted analysis of local factors contributing to ML activities.
- **Targeted Mitigation Measures** – By focusing on local contexts, sub-national assessments enable the development of tailored interventions and risk mitigation strategies that address the specific needs and challenges of communities, industries, or sectors within the area.
- **Community Engagement** – This approach involves local government, LEAs, businesses and community groups to foster good collaboration among key stakeholders and engagement in the risk assessment process.
- **Early Detection of Trends** – sub-national risk assessments may lead to the early detection of emerging ML trends and typologies within specific geographic areas, allowing the authorities to act quick and mitigate risks before they escalate to national level.

### Box A.2. Sub-national Risk Assessment

#### Germany

Germany's NRA is based on and builds on other risk assessments and sources, including the EU Supranational Risk Assessment (SNRA), sectoral or issue-specific assessments by federal authorities and the Länder, and input from the private sector and academia.

Following the NRA, the 16 German Länder (states) were tasked with conducting their own independent risk assessments. They identified regional differences, leading to different conclusions regarding the risk levels of certain sectors or products within each Land compared to the NRA's national level findings. For instance, while the NRA rated traders of goods, including art and antiques, as having a medium-high ML risk, Bavaria's assessment deemed the risk in the region low, considering market size, customer base, and transaction types. Some Länder assessments offered more nuanced perspectives on DNFBP risk than was provided in the NRA's analysis. Germany plans to bring together these findings to provide a national level understanding of the relative risks across sectors and regions.

Some considerations and challenges of the supranational and sub-national approaches are as follows:

- **Coordination** – All risk assessments may experience coordinating challenges, but this can be particularly the case in supranational and sub-national risk assessments. As stakeholders in these assessments may in some cases not have a relationship with each other, it is important that the entity leading the process ensures adequate support and coordination as part of the process. As with the NRA process, collaboration among such stakeholders may contribute to improving relationships across borders.
- **Loss of Local Specificity (Supranational) or National Level Breadth (Subnational)** – supranational risk assessments may focus less on risks that occur on a national level, as the purpose is often to understand and assess the global and cross-border risks affecting the group of countries for which the assessment is carried out. This would mean that the results do not necessarily consider country-specific contextual factors that impact the risk landscape and may at times lead to a lack of granularity in the risk assessment. It is to be kept in mind that the SNRA does not typically replace the requirement to conduct a risk assessment at a national level, and that the level of granularity required to develop a detailed understanding of risks is achieved through the country-specific risk assessment.
- **Dependency on External Risk Assessments (Supranational)** - Relying solely on external sources of information and expertise for risk assessments may result in a country adopting those methodologies, frameworks, and risk indicators. This does not allow for the country to adjust its approach based on its own risk and context.
- **“Ownership” of Process** - Some countries may see supranational risk assessments as encroaching on their right to manage their own risks, and not feel ownership of the process as it is managed by a supranational organisation. This is why early, and continuous engagement is needed to support collaboration. Similarly, sub-national assessments may struggle to engage local authorities and promote the necessity of risk understanding, particularly in areas with limited resources, capacity and risk-awareness.

## Annex B. High-level Summary of Responses to Public Consultation

1. **Question 1:** What are the most useful ways that the private sector, civil society, and academia can contribute to the NRA?

**Summary of Responses:** The most useful ways that the private sector, civil society, and academia can contribute to the NRA are regular forums and discussions, open surveys and consultations, participation in specialised working groups, collaboration with academic institutions on specific, in-depth research, and the provision of technical expertise and specialized advice.

Others identified include: Multi-sector collaboration between civil society associations, private organizations, and academia to work together to identify and assess emerging risks, drawing on their unique perspectives and experiences, complements the previous responses. Also, early engagement of the private sector at an early stage in the process would ensure that risk categories correspond to industry practices, allowing for granular and appropriate application of risk weightings.

2. **Question 2:** What are the most effective ways in which countries can engage the private sector, civil society, and academia in the NRA?

**Summary of Responses:** The most effective ways in which countries can engage that the private sector, civil society, and academia can contribute to the NRA are the setting up of educational workshops and seminars, and the planning of specific training sessions for the sectors concerned. The responses also highlighted the need to create digital platforms for the submission of feedback and reporting. Many also point to the need for collaboration with chambers of commerce and professional associations, as well as their active participation in the policy review process. All agreed on the need for a structured and continuous approach to collecting and responding to feedback.

3. **Questions 3:** How does the private sector, civil society and academia use NRA outputs? Are there any key performance indication or other methods to measure the impact of the NRA?

**Summary of Responses:** NRA outputs enable compliance and risk management policies, facilitate the improvement of training and awareness programs, and enable adjustments to be made to operational strategies of obliged entities based on the risks identified.

It should also be noted that they encourage the development of new initiatives to mitigate risks and promote the ongoing monitoring and evaluation of risks. NRA output encourage a range of training initiatives such as the implementation of learning programs based on identified risks, thereby improving awareness and preparedness in the face of threats. NRA outputs also form the basis of recommendations for policy updates, being used to update compliance and risk management policies based on recommended best practice.

4. **Question 4:** How can countries design NRA process and outputs to maximize their utility to the private sector, civil society, and academia?

**Summary of Responses:** The private sector recommends that countries design the NRA process in such a way as to encourage close collaboration with all stakeholders from the outset, enabling them to obtain clear and specific guidelines for compliance.



All stakeholders identified investing in capacity-building initiatives and the creation of practical tools and resources for risk management. Finally, all stakeholders called for transparency and access to NRA data and results for research to facilitate further research and better understanding of risks.

5. **Question 5:** Can you give concrete examples of how NRA findings have been used to improve your own risk management processes?

**Summary of Responses:** The results obtained for this question are largely consistent with the answers to question 3.

For a majority, the NRA findings have been used to improve their own risk management processes through the use of the results to update compliance policies by ensuring that practices are aligned with the latest risk management recommendations and the strict application of NRA findings in internal risk assessments.

NRA findings have also led to the strengthening of internal controls and audit procedures. The adoption of best practices recommended by NRA and the implementation of training programs based on identified risks are also recurring points.

6. **Question 6:** What is the most appropriate and effective mechanism for the private sector, civil society, and academia to provide feedback on the NRA?

**Summary of Responses:** Stakeholders recommend the creation of dedicated online portals for submitting feedback and the organization of regular consultation meetings. Stakeholders encouraged the publication of relevant information and ensure training for all those involved in the NRA.



[www.fatf-gafi.org](http://www.fatf-gafi.org)

November 2024

To establish a strong national AML (Anti-Money Laundering) framework, countries must prioritise a deep understanding of money laundering risks. This guidance document supports countries in conducting a money laundering NRA, drawing on insights from over 90 countries within the FATF Global Network.

