FATF

FATF TOOLKIT

Money Laundering National Risk Assessment Toolkit – Annexes A-C

August 2025

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**

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 (2025), Money Laundering National Risk Assessment Toolkit*,* FATF, Paris,

https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-National-Risk-Assessment-Toolkit-Annexes.html

Photocredits coverphoto ©

MONEY LAUNDERING NATIONAL RISK ASSESSMENT TOOLKIT – ANNEXES A - C

Acronyms

Acronym	Definition
AFA	Agence française anticorruption
AI	Artificial Intelligence
AML/CFT	Anti-Money Laundering/Counter Terrorist Financing
ATM	Automated Teller Machine
B2B	Business-to-Business
BO	Beneficial Ownership
CDD	Customer Due Diligence
CoE	Council of Europe
CRS	Common Reporting Standards
DeFi	Decentralised Finance
DNFBP	Designated Non-Financial Business or Profession
ECCD	Economic Crime and Cooperation Division
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FSRB	FATF-Style Regional Body
FUR	Follow-up Report
GDP	Gross Domestic Product
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
IDA	International Development Association
IDEA	Institute for Democracy and Electoral Assistance
IDR	Indonesian Rupiah
ILO	International Labour Organisation
IMF	International Monetary Fund
INR	Interpretive Note to Recommendation
IOSCO	International Organisation of Securities Commissions
ISO	International Organisation for Standardisation
KYC	Know Your Customer
LEA	Law Enforcement Agency
MER	Mutual Evaluation Report
ML	Money Laundering
MLA	Mutual Legal Assistance
NPO	Non-Profit Organisation
NRA	National Risk Assessment
OECD	Organisation for Economic Cooperation and Development
OSINT	Open-source intelligence
P2P	Peer-to-peer
PEP	Politically Exposed Person
PESTEL	Political, Economic, Social, Technological, Environmental, Legislative
PF	Proliferation Financing
POS	Point of sale
PSP	Payment services provider
R.	FATF Recommendation
RTMG	Risks, Trends and Methods Group

SAR	Suspicious Activity Report
SRA	Sectoral Risk Assessment
STR	Suspicious Transaction Report
TBML	Trade-based Money Laundering
TCSP	Trust and Company Service Providers
TF	Terrorism Financing
UN	United Nations
UNCAC	United Nations Convention Against Corruption
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organised Crime
USD	United States Dollars
VA	Virtual Asset
VASP	Virtual Asset Service Provider
VPN	Virtual Private Network
VRA	Vertical risk assessment

Box 1. Introduction to the Money Laundering (ML) National Risk Assessment (NRA) Toolkit

The topics of the following annexes to the ML NRA Guidance were selected because of a need for assistance identified in the Financial Action Task Force (FATF) Global Network. They should not be treated as a mandatory checklist or requirement, including because the FATF Standards do not require an NRA per se, nor do they specify a particular format of risk assessment product. The guidance document and its annexes are not an FATF Standard and are therefore not intended to designate specific actions necessary to meet obligations under Recommendation 1, the interpretative note to Recommendation 1 (INR.1), or any other FATF Standards. Criteria for technical compliance and for assessing effectiveness is only 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.

Countries do not have to go through each of the annexes or guides but can elect to use the materials that are relevant and appropriate in their own unique risk and context. If a country, considering its risk and context, sees a need for a specific risk assessment or a chapter on (for example) corruption, it can consult the relevant quick guide to assist in this work.

The suggested sources listed for data are non-exhaustive and should not replace data collection and analysis on a national level. Rather, the goal is to provide a variety of sources for background information that can support jurisdictions in the initial stages of research on their risks. It is recommended that countries assess the reliability of all sources used and do not take external data sources at face value, rather use them to supplement their national level data and risk understanding, especially where there are data gaps.

The NRA process should be kept manageable and the resulting document of a reasonable length to remain accessible and useful to both the public and private sectors.

Countries should note that these annexes should be read in conjunction with the ML NRA Guidance as they complement and supplement the information therein. These annexes do not discuss every stage of the NRA process; where there is no specific supplementary guidance or information provided, countries are invited to refer to the information in the ML NRA Guidance document.

Examples of NRAs and other risk assessments can be found on the RTMG Community site (link not public).[1] This page is updated regularly when the FATF Secretariat receives notice of newly published risk assessments.

Annex A: Quick guides for assessing challenging areas of risk assessments

1. This annex is designed to help countries address challenging areas of risk assessments by providing practical advice that countries can implement to help them to enhance the effectiveness of their ML risk assessments. Countries should always ensure they adapt these tools to their specific risk and context, and go beyond them, as needed.

2. As mentioned in the ML NRA Guidance, countries should do an environmental scan of all ML threats and vulnerabilities present before proceeding to analyse them. Countries are encouraged to note in their NRA or other risk assessments which areas are emerging risks or where there is some awareness about a risk, but limited data or information as to its scope, or frequency of occurrence. The areas below have been chosen as they have consistently proven challenging to assess, often because of limitations faced in obtaining data or the level of understanding of the sectors exposed to those risks and how they can be mitigated. Concluding that there is not enough data or information available to accurately assess risk in a particular area is also valuable, as it can inform a country's action plan, and support prioritisation of further work to improve risk understanding for future NRA iterations, enhance data collection, or to support the commencement of a sectoral or thematic risk assessment.

3. These annexes include selected good practices from a variety of countries across the FATF Global Network and have been drafted with the aim of providing common steps that countries can apply regardless of their specific context, maturity of risk assessment process, the complexity of their anti-money laundering (AML) system, etc.

4. The four topics discussed in Annex A are:

- Corruption
- Virtual Assets (VA) and Virtual Asset Service Providers (VASP)
- Legal Persons and Legal Arrangements
- Informal Economy

5. It is important to assess these areas in such a way that the findings can be integrated into other work taking place in the country to improve risk understanding.

[1] Library of ML/TF/PF Risk Assessments (a accessible to FATF delegations).

Countries should decide, based on their risk and context, how to best assess their risks. The risk assessment of these areas could be incorporated into a country's NRA, done as a separate thematic/sectoral risk assessment, or examined as part of other risk assessment work (e.g. typologies reports). The extent of the informal economy and levels of corruption in the country could be considered as contextual factors, which impact various threats and vulnerabilities and can impact the overall risk levels in the country. Given that VA/VASPs and legal persons and arrangements intersect with many other areas of ML risk and have proven challenging to assess, countries may decide to do a "deeper dive" as part of a sectoral/thematic risk assessment, even if they have already included these topics in their NRA, to enhance their risk understanding.

6. There are often links between these topics, and the sections below note data and factors from other topics that could be considered to gain a deeper understanding on risk. Examples may include:

- Corrupt officials may exploit their positions to siphon government funds and use shell companies to disguise the origin and movements of funds.
- Funds from corruption could also be converted into VA to disguise the origin of funds and facilitate cross-border transfers.
- Professional enablers could establish legal persons or arrangements to enable or facilitate the transfer of funds to public officials, paid as bribes in exchange for the reward of public or government contracts.
- Criminals can take advantage of the informal economy through purchasing materials from unregistered businesses, over-invoicing the goods, and then using shell companies to launder the funds. Shell companies may also be abused for tax evasion purposes, tax evasion being a driver for informal economy.

7. It is therefore important that when conducting assessments of these topics, that countries consider possible links to other sectors and risk areas, and how these may affect the scope and impact of the risks under assessment. Countries are encouraged to consider these risks within the context of other possible risks, rather than assessing them in isolation to one another. The links between these topics also show that it is important to consider the context of the country and the broader environment in which ML takes place to fully understand the risks. Any action plans that arise from the findings of the NRA should consider the possible existence of these links in the country. Risk areas being linked and overlapping could increase risk levels, but it could also mean that countries can use the measures for mitigating one risk to mitigate the risks of a linked risk.

Quick guide on assessing the ML risks of corruption

Box 1. Corruption statistics at a glance

- The FATF's report on the State of Effectiveness and Compliance with the FATF Standards identified corruption as the second most common major proceeds-generating predicate offence posing ML risk identified in MERs.[2]
- World Bank research on 147 MERs from the Global Network found that corruption was the main predicate offence for 34 countries, and in the top five predicate offences for 128 countries.[3]
- In 2018 the United Nations (UN) estimated that every year, roughly 3.6 trillion USD, equivalent to more than 5% of global gross domestic product (GDP), is paid in bribes or stolen through corruption.[4]

8. Corruption features in most countries' NRAs in some form (e.g., as a threat, or contextual factor). However, some jurisdictions may need to complete more in-depth analysis on corruption and ML risks derived from corruption, as seen from countries' MER results, key findings and recommended actions.

Table 1. Considerations when assessing ML risks of corruption

To assess the ML risks of corruption, countries could consider the following:[5]

Consideration	Reasoning and comments
Analyse country context	Regarding the risk of corruption in the country: • Relevant legal and regulatory contextual issues specific to the country. • International corruption threats and regime vulnerabilities that the country faces, including United Nations Convention Against Corruption (UNCAC)[6] implementation review mechanism reports[7] and country profiles,[8] where available, and analysis of the

[2] FATF (2022), *Report on the State of Effectiveness Compliance with FATF Standards*, p.14.

[3] Unpublished World Bank research, 2024.

[4] UN (2018), retrieved from https://news.un.org/en/story/2018/12/1027971 (accessed 17 January 2025).

[5] The suggested sources listed for data are non-exhaustive and should not replace data collection and analysis on a national level. Rather, the goal is to provide a variety of sources for background information that can support jurisdictions in the initial stages of research on their risks. It is recommended that countries assess the reliability of all sources used and do not take external data sources at face value, rather use them to supplement their national level data and risk understanding, especially where there are data gaps.

[6] UNODC, UNCAC – *United Nations Convention Against Corruption*, www.unodc.org/corruption/en/uncac/index.html (accessed 2 April 2025)

[7] UNODC, *UNCAC Implementation Review Mechanism*, www.unodc.org/corruption/en/uncac/implementation-review-mechanism.html (accessed 2 April 2025).

[8]. UNODC, Country Profiles, www.unodc.org/corruption/en/country-profiles/view/search.html (accessed 2 April 2025).

effectiveness of anti-corruption laws and AML responses in law enforcement agencies (LEAs) and supervisory agencies.

- Wealth from extraction of natural resources, such as oil and timber in absence of good governance may make some countries more vulnerable to corruption at the highest levels of government.[9]
- Prevalence of the informal economy in the country.[10] [11]
- Consider the different ways corruption manifests itself, e.g., as a predicate offence or as a contextual factor that can increase a threat because of its role in facilitating other types of crime. Corruption can be facilitated and enabled by certain conditions in a country, e.g., poor working conditions of public officials.
- Examine the extent of digitisation in procurement, work processes and documentation, including online systems that enhance efficiency, accountability, transparency, and create an audit trail; the public availability and accessibility of citizen charters detailing government commitments; and the population's literacy level along with public awareness and participation in governmental policies and their execution.
- Countries should consider the extent of corruption in both public and private sectors which may be relevant to ML risks. In some cases, public and private sector corruption may be linked, and be facilitated or exacerbated by similar factors.
- Rule of law, independence of judiciary and freedom of the press, particularly in coverage of new stories related to corruption.
- Examine role of state capture, which is broader than other forms of corruption. It may involve activities that are not illegal, such as shaping laws to benefit those in power and undermining the activities of key AML agencies. Recognising that assessing the level of state capture in their own jurisdiction may be challenging, countries could build contextual understanding by looking at countries with similar profile or other countries in the region.[12]

Regarding Politically Exposed Persons (PEPs):

- Identify PEPs (foreign and domestic).
- Examine the effectiveness of oversight of PEPs.
- Examine PEP use of legal persons and arrangements.
- High-value transactions and unexplained wealth.

Regarding proceeds and types of corruption:

[9] FATF (2012), *Specific Risk Factors in the Laundering of Proceeds of Corruption*

[10] See also Table 5 in the *Quick Guide on Assessing ML Risks of the Informal Economy* in Annex A.

[11] The relationship between corruption and the informal economy is debated by academics. Some argue they are substitutes—informal activity arising to avoid corruption and overregulation (Schneider & Enste, 2000; Djankov et al., 2002; Choi & Thum, 2005; Dreher & Schneider, 2006). Others see them as complementary, especially in contexts with weak institutions, where both tend to reinforce each other (Johnson et al., 1997; Buehn & Schneider, 2009; Dreher & Schneider, 2010; Ouédraogo, 2017; Bayar et al., 2018). The consensus suggests the nature of this relationship is context-dependent, in countries with weak institutions and governance, corruption and the informal economy often reinforce each other, whereas in countries with stronger regulations and lower tax rates, they may serve as substitutes.

[12] Results for Development (2024), *State Capture Matters: A research article and associated dataset and index*, https://r4d.org/resources/state-capture-index/ (accessed 20 May 2025)

	• Identify proceeds generating offences that involve corrupt activity e.g., embezzlement and extortion. • Identify enablers and funding channels i.e., where does the money go once it has been obtained? • Explore typologies used for laundering proceeds of corruption. The FATF's 2011 Report on Laundering the Proceeds of Corruption,[13] which considered the work of anti-corruption bodies, provides explanations, definitions and typologies that explain the uniqueness of corruption vs. other offences, e.g., crimes where the offender may be in a privileged position or position of power that allows them to launder funds more easily. • Some common typologies include large unexplained cash deposits or withdrawals by PEPs; and the use of corporate vehicles and trust or nominees, trusted associates or family members which in itself may be legitimate but can still have an impact on customer due diligence (CDD) controls.[14] • Consider all types of corruption present in the country (e.g., small scale, grand corruption, public sector, private sector, is it widespread, which sectors/populations are vulnerable to corruption, and do they understand the risks? Does this contribute to state capture?). • Pay particular attention to proceeds of grand corruption in government procurements, such as large infrastructure projects, as the total loss can be significant. Regarding foreign corruption: • Consider the risk and context of the wider region, as well as that of countries with similar risk profiles, and those in the same regional economic integration organisation. • Consider the nexus between international cooperation and corruption. Countries that are more exposed to domestic corruption may also be more at risk from exposure to proceeds of foreign corruption. On the other hand, even countries with low risks of domestic corruption may have high risks of the proceeds of foreign corruption entering the country for laundering, e.g., in cases where neighbouring countries are known to have high rates of corruption. • Endeavor to understand the risks of financial flows either entering or leaving their financial system from and/or to countries perceived as high-risk with regards to corruption and of foreign PEPs.
Process and drafting	Once inherent risk is assessed, the effectiveness of mitigation measures, including administrative controls that are more aimed at increasing transparency, can be considered to assess residual risk. It is important to empower and protect stakeholders working on the risk assessment to help ensure the accuracy and reliability of the assessment and there are no consequences to those working on the assessment for negative findings. Countries could consider including the following stakeholders: • Public sector: anti-corruption agencies, Financial Intelligence Units (FIUs), LEAs, public procurement authorities • Private sector: banks, auditors, anti-corruption non-profit organisations (NPOs) and civil society organisations
Data sources	Countries could consider the following data sources to support their risk assessment. This list is non-exhaustive:

[13]. FATF (2011), Laundering the Proceeds of Corruption

[14] Ibid, pages 17 -25.

	Related to corruption as a predicate offence or contextual factor: • Types of PEPs present in the country where available (e.g., for example, where countries have a list of position/functions that constitute PEPs)[15] and beneficial ownership (BO) registries showing the interests of PEPs. • National, regional and international studies on corruption produced by governments and the public sector. Reports by international organisations, e.g., FATF, FATF-Style Regional Bodies (FSRBs), Organisation for Economic Cooperation and Development (OECD), UN Office on Drugs and Crime (UNODC). • National and international corruption perception indexes, e.g., World Bank's corruption perceptions index,[16] World Bank's Enterprise Surveys – Corruption Perceptions,[17] the International Development Association (IDA) Resource Allocation Index which provides ratings on transparency, accountability and corruption in the public sector,[18] the International Institute for Democracy and Electoral Assistance (IDEA): Political Finance Database which measures "absence of corruption",[19] and other such tools which can be used to understand and mitigate corruption risk. These sources should not be taken at face value but can be useful in providing background context and ideas for further research. • Reports and investigations undertaken by national anti-corruption bodies, NPOs or civil society concerning campaign financing disclosures and conflicts of interest declarations by public officials. • Data from LEAs on investigations, prosecutions and convictions for corruption and related offences, including violations of PEP regulations. Redacted reports received via whistleblower hotlines. • Academic research and objective press reports.[20] Interviews with subject matter experts. These can help countries identify blind spots but should not be taken at face value and instead can support a country in developing its own understanding and conclusions. • Aggregate public procurement data (combined with tax information and financial intelligence) can be analysed for red flag indicators, e.g., the percentage of tenders awarded to legal persons created in the period just before tender announcements (a high percentage could suggest that tenders were prearranged), links between procurement data with suspicious transaction reports (STRs) filed and tax discrepancies - a red flag indicator could be companies that have not declared any revenue to the tax authorities being awarded contracts. Misuse of legal persons may be more common in certain sectors than

[15] See FATF's definition of PEPs in the Glossary to the *FATF Recommendations* and the FATF *Guidance on Politically Exposed Persons* (2013). As indicated in the Guidance, compiling and maintaining a list of domestic positions/functions may not be overly onerous for individual countries. In fact, many countries already have a list of public functions that are required to file asset disclosures, which are likely to remain consistent for a period of time and where occasional updating would be sufficient.

[16] World Bank, *Corruption perceptions Index,* available at: https://data.worldbank.org/indicator/IQ.CPA.TRAN.XQ (accessed 2 April 2025).

[17] World Bank, *Enterprise Surveys – Corruption Perceptions,* available at: www.enterprisesurveys.org/en/data/exploretopics/corruption (accessed 19 May 2025).

[18]. IDA, *Resource Allocation Index,* available at: https://ida.worldbank.org/en/financing/resource-management/ida-resource-allocation-index (accessed 2 April 2025).

[19]. IDEA, *Political Finance Database,* available at: www.idea.int/democracytracker/about-the-gsod-indices (accessed 2 April 2025).

[20]. For example, the Organised Crime and Corruption Reporting Project, available at: www.occrp.org/en (accessed 3 April 2025)

others, so countries can consider whether there are differences in sectoral vulnerabilities.

- Cases of abuse of regional assistance programmes (such as the Recovery and Resilience Plans[21] funded by the European Union, or the UN development group resilient recovery support to Latin American countries).[22]
- Objective press reports and independent, investigative journalism can provide useful background information and context.[23]
- Interviews with academics, interviews with subject matter experts and NPOs conducting evidence-based research into corruption or ML from corruption.

Related to ML from corruption:

- STRs and cases from LEA and prosecutors, including any involving PEPs and their associates and unexplained wealth.
- Mutual Legal Assistance (MLA) requests from foreign jurisdictions related to corruption and the laundering of the proceeds. STRs related to corruption and ML in foreign jurisdictions obtained from counterpart FIUs.
- National, regional and international studies on corruption and ML. Reports by international organisations (e.g., FATF, FSRBs, OECD, UNODC).
- Data from LEAs on investigations, prosecutions and convictions for ML related to proceeds of corruption and related offences, including those involving shell companies. Confiscation data related to corruption.
- World Bank's "Control of Corruption"[24] statistics provide an objective assessment and cross-comparison of state of corruption in a country. The World Bank's other governance indicators such as on "Rule of Law," "Governance Effectiveness," and "Regulatory Quality" can also provide valuable and objective insights also during the ML risk assessments.
- Consider the possibility of undetected cases which may impact the country's risk ratings, especially when there is little data available. Detected cases are sometimes only the tip of the iceberg. Countries can leverage other sources such as international reports, data obtained from other countries, corruption perception indexes to supplement the data they collect domestically to give a broader picture of the possible risks.

[21]. European Commission, *Recovery and Resilience Plans*, https://reform-support.ec.europa.eu/what-we-do/recovery-and-resilience-plans_en (accessed 2 April 2025)

[22] UN Development Group, *Resilient Recovery*, www.undp.org/latin-america/resilient-recovery (accessed 2 April 2025)

[23] Countries are encouraged to have multiple independent sources, ensure not to use media funded by special interest groups or biased reports from nationally controlled media.

[24] World Bank, *Control of Corruption Statistics*, http://info.worldbank.org/governance/wgi/ (accessed 14 April 2025)

Box 2. Corruption risk assessment case studies

In 2019, Indonesia and Malaysia jointly led a new ML work stream within the Financial Intelligence Consultative Working Group to assess the regional[25] threat of transnational laundering of corruption proceeds. This assessment examined corruption-related ML within and beyond the region, aiming to provide actionable information to enhance cross-border collaboration. It focused on key areas such as the cross-border movement of corruption proceeds, typologies of crime and laundering methods, and country self-assessments on threats, vulnerabilities, and countermeasures. Emerging risks, such as VA, were also considered.

The assessment used quantitative and qualitative data from 2016-2018, drawing from sources like STRs, international fund transfers data, international exchange of information, investigations and prosecutions data, case studies, typologies reports, research papers and consultations with stakeholders such as anti-corruption agencies in the region. Findings highlighted that corruption proceeds are typically laundered through banking services, and commonly involved legal persons, while the abuse of trusts (including offshore trusts) is also noted. Larger-scale corruption cases involved sophisticated schemes using complex legal person structures and multi-jurisdictional layering. While emerging threats like VA were not prevalent, they are acknowledged and will continue to be monitored.

Source: Indonesia and Malaysia

In 2024, the French anti-corruption agency (AFA) published an analysis based on the examination of 504 first-instance court decisions handed down between 2021 and 2022.[26] These decisions, although not final for some (as they can be overturned on appeal or annulled in cassation), constitute a robust methodological basis for analysing breaches to probity in France. AFA's analysis offers a better understanding of sectoral and geographical areas of vulnerability and identifies fraudulent patterns to anticipate and detect risks. France structured its study around an in-depth analysis of the judgments transmitted by the criminal courts. Each decision has been documented by taking into account several characteristics:

- Offences identified (e.g., corruption, embezzlement and undue favouritism)
- Profiles of the defendants (e.g., age, position, profession and geographic area)
- Description of the corruption scheme
- Consequential legal procedures (e.g., nature of sentences, appeal rate and duration of proceedings)

This methodology is based on an exhaustive and territorially representative corpus, making it possible to draw up a precise map of corruption risks in France. The findings showed that some sectors appear to be exposed to greater risk than

[25] Countries included: Australia, Brunei Darussalam, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, New Zealand, Philippines, Singapore, Thailand and Vietnam.

[26] . Agence Française Anti-corruption (2024), *Note d'analyse 2024,* Note_Analyse_Decisionsdejustice_ObservatoireAFA_09122024.pdf

others: in the public sector local authorities account for 50% of offences (municipal block in particular) in particular acts of favouritism and illegal acquisition of interests. In the private sector the construction, scientific and technical sectors are among the most exposed. Moreover, some regions have a higher incidence of breaches regarding probity. These disparities are nuanced according to the type of offence (e.g., corruption, embezzlement or illegal acquisition of interests).

Source: France

A typologies study on ML through corruption was conducted in 2020 by Gambian AML experts, in collaboration with the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA). The study assessed the adequacy of the legal, regulatory and institutional frameworks in The Gambia, the efficacy of the judicial systems in combating corruption, and how corruption compromises the effective implementation of AML measures in The Gambia. In addition, the main methods of ML of the proceeds of corruption were also assessed.

There is a strong focus on the risk and context of this country. Corruption is one of the key predicate offences to ML in The Gambia and the report explores the history of corruption in the country and possible reasons for it being so rife (e.g. low morale in LEAs due to low salaries and limited powers and material resources to do their job).

The data sources used for this study are varied and include results of a perception survey of corruption in The Gambia that was sent to the general public, media reports and allegations of corruption. It mainly focuses on corruption in the public sector, as corruption in the private sector is not discussed in media unless it links with bribes to senior public officials or politicians.

The report analyses the change in perceptions of corruption and typologies over the years and possible reasons for this. The study includes case studies (which include cases related to former high-level politicians and their families) and red flag indicators for each typology.

Source: The Gambia

Quick guide on assessing the ML risks of virtual assets (VA) and virtual asset service providers (VASP)

Box 3. VA/VASP risk assessment statistics at a glance

- Based on MER findings, only 15 out of the 137 jurisdictions are rated fully compliant with the requirements of criterion 15.3. Seventy percent (96 out of 137) of jurisdictions assessed on R.15 are not sufficiently implementing the requirement to conduct a risk assessment on VA/VASP. This aligns with the results of the FATF's March 2025 survey of the global network on the implementation of R.15, in which a quarter of respondents (39 out of 163) reported that they had not conducted a risk assessment on VA/VASPs.[27]
- A common deficiency found under c.15.3 was a gap in the scope of the risk assessment, i.e., the country's definition of VASP is not in line with FATF's definition and therefore the risk assessment was not considered comprehensive.
- Responses to the FATF's October 2023 survey from the update of the ML NRA guidance project showed that over 28% (17 out of 60) of responding delegations reported difficulties in assessing the risks of VA/VASPs, and 17% (10 out of 60) reported difficulties assessing the risks of new and emerging technologies in general, which may include VA/VASPs.[28]
- The FATF's 2024 Targeted Update on the Implementation of the FATF Standards on VA and VASPs found that ML associated with VA, particularly proceeds from VA theft, fraud and scams often involves anonymity-enhancing coins, mixers, Decentralised Finance (DeFi) arrangements, and cross-chain bridges.[29]

9. According to the FATF's 2025 Targeted Update on the Implementation of the FATF Standards on VA and VASPs, although there has been some progress with compliance, many jurisdictions still struggle with the implementation of some of the fundamental requirements of R.15, particularly undertaking a risk assessment on VA/VASP.[30]

10. When undertaking a risk assessment related to VA/VASPs, countries should consider how VASPs differ to traditional financial institutions (FIs), and how and to what extent VA/VASPs interact with the traditional financial and non-financial sectors. The table below explains some key differences between VA/VASPs and traditional fiat currencies and FIs.

[27] FATF (2025) Targeted Update on Implementation of the FATF Standards on VA and VASPs, 2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf, Figure 1.4.

[28] Survey was in relation to the update of the ML NRA Guidance.

[29] FATF (2024) *Targeted Update on Implementation of the FATF Standards on VA and VASPs,* 2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf, paragraph 45.

[30] Ibid., Key Findings.

Table 2. Key differences between VA/VASP and traditional fiat currencies and FIs

Topic	Fiat currency/Traditional FI	VA/VASP
Regulation	Generally, a heavily regulated sector with broader focus (e.g., prudential requirements and consumer protections). There are international bodies that impose regulations that are consistent across borders (e.g., the Basel Framework).[31]	Regulation varies per jurisdiction. Sector may be completely unregulated in certain jurisdictions, newly regulated for AML/CFT purposes or have transitioned from "light touch" to more comprehensive regulation.
Anonymity	Cash can be exchanged anonymously, but transactions through traditional FIs are generally tracked and recorded.	VA has perceived anonymity as user identities are not recorded on the blockchain, and anonymity enhancing services such as tumblers, mixers,[32] chain swapping or cross-chain bridges[33] make it more challenging to trace the origin and destination of funds. Some types of VA are configured to facilitate anonymity of the holder, making it difficult to trace the originator of a transfer. Lack of implementation of the Travel Rule and transmission of information on the originator and beneficiary of a transfer also reduces available information for conducting due diligence and screening on transactions and hampers LEA investigations.
Security	There are generally stronger protections for customers of traditional FIs. Banking systems tend to be more established and secure (however there is still some risk of data leaks and hacking).	Certain transaction details on many public blockchains are transparent, visible and immutable. Initial coin offerings, promoting fund-raising in support of an VA, can be vulnerable to exploitation through insider manipulation in the form of "rug pulls".[34] Security systems may be less established and secure, particularly when there is little or no regulation. Use of personal keys to access VA and authorise transfers, which can be done via a VASP or directly between transferring parties, can be lost or stolen Infrastructure of VASPs is vulnerable to cyberattacks and hacking, and customer data may not be well safeguarded.
Access	If sufficient AML measures are in place, to open an account, documentation including identification is required. Know-your-customer (KYC) checks and due diligence may be undertaken by the bank before opening an account, and continual checks may be done to adhere to AML obligations.	Easily accessed through the internet regardless of location. Unregulated VASPs may not require identification or KYC checks and ongoing due diligence (or if they do, they may not be adequate) to open a wallet or access the wallet to make transfers. VAs may be transferred through peer-to-peer (P2P) trading platforms through self-hosted or self-hosted wallets, which are not subject to identification or KYC checks and ongoing due diligence.
Data	FIs have generally been subject to ML reporting requirements for a long time, have more experience submitting STRs and interacting with government agencies engaged in AML efforts.	VASPs may not be reporting entities, or may only recently have become reporting entities, which means that regulatory data may not be made available to authorities in a standard format (e.g., it doesn't align to STR formats) and may be more difficult to analyse. VASPs which operate in unregulated jurisdictions are not required to submit STRs. VASPs maintain transfer activity data incorporating transaction hashes and blockchain data, which requires additional training and expertise for investigators and law enforcement to analyse.

[31] Bank for International Settlements, www.bis.org/basel_framework/ (accessed 27 January 2025).

[32]. Tumblers and mixers are services that use various methods to conceal the connection between the address sending VA and the addresses receiving VA. Depending on the products and services offered, these entities themselves may be VASPs.

[33] Chainalysis (2024), *Introduction to Cross-Chain Bridges*, www.chainalysis.com/blog/introduction-to-cross-chain-bridges/ (accessed 7 May 2025)

[34] Chainalysis (2021), *Crypto Scams: 2021 Rug Pulls Put Revenues Near All-Time High*, Crypto Scams: 2021 Rug Pulls Put Revenues Near All-Time High (accessed 30 April 2025)

Types of assets involved	Fiat currencies are government-issued legal tender, often offering stability as government backed. However, fiat currency can also lose much of its value, e.g., during a financial crisis. Fiat currency is susceptible to inflation or hyperinflation.	VA can include cryptocurrencies (e.g., Bitcoin), tokens, non-fungible tokens etc., either with or without a centralised issuing authority. They can fluctuate significantly in value and may have little or no customer protection or compensation measures. VA can be susceptible to volatility, price uncertainties and liquidity issues, with challenges to accurately assessing their actual value. VA can include products that are complex and difficult to verify as to their authenticity or operability once developed.
Tax	Taxable events in fiat currency are well-established. Banks and employers typically report directly to the tax authorities. The high traceability and oversight of fiat currency through regulated FIs makes it easier for tax authorities to enforce compliance and more difficult to evade tax. As mentioned in Annex B of this document, tax crimes are frequently cited as one of the "top four" predicate offences to ML.	VA transactions may be subject to taxation (e.g., capital gains tax, income tax or VAT) depending on the country's tax laws. Some countries classify VA as property or commodity, and some as currency, which may influence the transparency around the size and value of VA held or transferred for tax purposes. VA may be susceptible for misuse by parties seeking to evade tax or engage in other tax crimes, given the possibility of concealing the owner or controller of VA or concealing the true wealth or income otherwise declarable by individuals or legal entities.[35] Legal and regulatory frameworks needed to implement tax transparency measures for VA and VASPs, as developed by the OECD, including the automatic exchange of tax information on transactions in VA between countries ("Crypto-Asset Reporting Framework")[36] may not yet have been introduced by some countries or incorporated as part of existing taxation reporting and oversight requirements.[37]
Transaction/transfer processing	Transactions through FIs are centralised and may involve intermediaries (e.g., payment service providers (PSPs)) However, cash movements are not centralised and can involve direct P2P operations (e.g., hawala networks).	Transfers made using VA occur using blockchain technology, which may be through a distributed network with varying levels of verification concerning the transfers made on the chain. Transfers may be undertaken on a P2P basis or using a P2P platform,which may not verify the identity of originators or recipients of transfers or the origin of the funds or proceeds used to acquire the VA transacted. Transfers can be undertaken rapidly and cannot be "rejected" or reversed, for example if financial crime risks are detected through sanction screening.
Cross-border transactions/transfers	Transactions can be expensive and slow due to intermediaries and currency conversion fees. Transactions can involve intermediaries such as correspondent banks that apply AML measures to both the sending parties and the transactions involved.	Transfers can be almost immediate as sometimes no intermediaries are used. VA transfer fees are also generally low or non-existent. VASPs can conduct VA to VA transfers without using correspondent banking services. VASP transfers can involve different intermediary VASPs, operating across several jurisdictions, with varying AML regulatory requirements.

11. Countries that decide to prohibit or limit VA/VASPs should still understand the ML risks associated with them and any unlicensed activity. Countries should have a detailed decision-making process evidencing the basis upon which it has adopted its approach towards addressing ML risks linked to VASPs. This can include outright prohibition, restricted permissible VA/VASP activities or the application of an VA/VASP authorisation process. It should include the analysis undertaken to assess the impact the chosen approach could have on the possible ML risks linked to

[35] IMF (2023), *Crypto Poses Significant Tax Problems—and They Could Get Worse*, www.imf.org/en/Blogs/Articles/2023/07/05/crypto-poses-significant-tax-problems-and-they-could-get-worse (accessed 27 April 2025)

[36] OECD (2023), *International Standards for Automatic Exchange of Information in Tax Matters,* www.oecd.org/en/publications/2023/06/international-standards-for-automatic-exchange-of-information-in-tax-matters_ab3a23bc.html

[37] Although increasingly VASPs are required to report trading of VA, often information is self-reported information by the individuals taking part in the trading of VA.

VA/VASPs operating in or from the country. It should also consider that the risks associated with the sector and ability to enforce such a prohibition or limitation may evolve rapidly, and a plan to continue to assess the risks, including emerging risks, on an ongoing basis.

12. Regardless of whether a country decides to prohibit VA/VASP activity, additional risk mitigating measures may be necessary, including identifying VASPs that operate illegally in the jurisdiction, assessing the risk of VA/VASP services offered in the country by a VASP based abroad, and applying proportionate and dissuasive sanctions to such entities. Based on a country's risk profile, restricting VA/VASP activity through either a prohibition or activity restrictions should also be supported through ongoing mitigating measures such as outreach to the private sector about such risks and enforcement actions where such restrictions are not complied with and risk-mitigation strategies that account for the cross-border element of VA activities and VASP operations.[38]

13. This annex contains a non-exhaustive reference guide table with suggested areas for assessing the ML risks linked to VA/VASPs, followed by some case examples from countries that have done a VA/VASP risk assessment.

Table 3. Considerations when assessing ML risks of VA/VASP

To assess the ML risks of VA/VASP, countries could consider the following:[39]

Consideration	Reasoning and comments
Analysis of both VA and VASP in the risk assessment	Often, countries assess the risks of VA and VASPs in the same document, whether as part of the NRA or a sectoral risk assessment. Countries must be sure to consider the risks of both and consider the linkages between them in their risk assessments. Firstly, countries may wish to understand the types of VA that are present and how they function and are used for both legal and criminal purposes. Then, countries can analyse VASPs - for example their customer base, the types of VA services that they offer, existence of foreign incorporated VASPs in the jurisdiction, existing regulations and controls and their effectiveness, and the vulnerabilities that exist in the sector.
Ensure the appropriate authority leads the assessment	Countries should choose the appropriate authority to lead the risk assessment of VA/VASPs considering its particular circumstances. In some cases, a central authority which is neither the FIU nor the supervisor is best-placed to lead this risk assessment. There are benefits to having the FIU and lead VASP supervisor involved in the VA/VASPs risk assessment, whether it is part of an NRA or a separate sectoral risk assessment, even if they do not lead it, given the data and expertise they have access to. FIUs: • The FIU is at the centre of the national AML/CFT framework and is in a unique position when it comes to VA/ VASP due to its ability to detect unlicensed and suspicious activity via STRs filed by banks or other reporting entities which may come into contact with VA/VASP activity, even if VA/VASP activity is prohibited in the jurisdiction. • FIUs are specialists in analysing financial data, making them well-suited to identify vulnerabilities in the financial system that could be exploited

[38] For more information, see FATF (2012), *Updated Guidance for a Risk-Based Approach for VA and VASPs*, This paragraph is taken from paragraph 109 of this guidance.

[39] The suggested sources listed for data are non-exhaustive and should not replace data collection and analysis on a national level. Rather, the goal is to provide a variety of sources for background information that can support jurisdictions in the initial stages of research on their risks. It is recommended that countries assess the reliability of all sources used and do not take external data sources at face value, rather use them to supplement their national level data and risk understanding, especially where there are data gaps.

	for ML, including through VA/VASP. • FIUs facilitate information sharing between national authorities and often have established relationships with FIUs in other countries, aiding international cooperation, gathering information, and sharing of best practices regarding VA/VASP risk assessment and emerging typologies and risks. VASP supervisor: • VASP supervisors can provide information and data on the VASP sector, e.g., sector-wide risk trends and red-flag indicators, volumes of VA transfers, geographic risks, emerging ML risks related to VA/VASP, compliance data, and typologies for abuse of the sector. • They can flag broader vulnerabilities of the sector in the country as they are involved in assessing compliance of VASPs. They know where there are regulatory gaps or deficiencies in compliance. Countries could consider including the following stakeholders: • Public sector: Financial sector and VASP supervisors, FIUs, LEAs, Central Banks, technology and fintech regulators, cyber security authorities. • Private sector: VASPs, VA exchanges, academics, fintech associations, cyber-security companies and blockchain analytics companies.
Establish the country's context	A scoping exercise of the VA/VASPs that are present and operating in the country is recommended to develop a picture of the extent and nature of VA/VASP activity. For a VA/VASP risk assessment it is beneficial to start with an overview of the general risk landscape in the jurisdiction to establish a picture of the level of VA/VASP activity and related frameworks that exist concerning these sectors. Examples of information that could be including in describing the VA/VASP context in a country could include, but not be limited to: • The main types of VA/VASP products and services used and operating in the jurisdiction • Breakdown of VA/VASP activity in terms of licensed or registered VASPs vs. estimated unlicensed or unregistered activity. Prescence of foreign VASPs in the jurisdiction.[40] • Breakdown of the types of legal persons operating as VA/VASPs in and from the country, including the number of legal persons established, controlled or owned by parties outside of the country; breakdown of the number of active legal persons operating as VA/VASPs as compared to those no longer active or dissolved. • Regulatory gaps in the jurisdiction, including gaps in the scope of VASPs that are covered (refer to FATF definition of VASPs in the glossary of the FATF Standards). • Appetite of local population for VA/VASP products, evidenced by levels of known activity and most frequently accessed types of products. • Prevalence of use of VA as currency for payments or for investment. • Size of VA/VASP market activity in the country relative to activity taking place in the region and globally. • What licensing and registration processes have been put in place for the sector? Identify potential drivers of VA/VASP presence in the jurisdiction, e.g., speed and ease of legal person incorporation, absence of AML/CFT framework for VA/VASPs, lack of tax obligations on VA transfers and innovation-positive economy. Comparisons with other countries may show evidence of regulatory arbitrage which can develop contextual understanding for the risk assessment.

[40] It is important to note that VA/VASP are cross-border in nature, and so even if VA/VASP activity is prohibited in the country, VA services and products hosted in a foreign jurisdiction may be offered online.

	• Levels of financial inclusion, since low levels of financial inclusion may lead to higher uptake of VA. • Detectable transfer flows (i.e., receives/sends transfers, is a conduit for onward transfer activity, used for conversion of VA to fiat, mainly handles VA to VA transactions etc.) • Interrelationship between VA activity and other regulated entities – e.g., use of banks, use of payment service providers (online) and use of money service / remittance providers. • A summary of the predicate offences analysed in the last NRA or other risk assessment activity to enable comparison when predicate offences are assessed in relation to VA/VASPs later in the process.
Analyse threats and vulnerabilities	Consider the key components of risks, threats and vulnerabilities, preferably separately. Countries should explore the linkages between VA/VASP activity and key predicate offences and vulnerable sectors, e.g., VA/VASP used in ransomware or fraud cases to support the crime, artificial intelligence (AI) to help criminals navigate using VA and possible abuse of VA in the Metaverse, on social media platforms or the dark web. For VAs: • Consider features that may make them attractive to criminals, and therefore vulnerable for abuse for ML (i.e., the factors driving a criminal to elect one VA over another for ML purposes). • Consider threats arising from the extent of illegal activities carried out on or facilitated by the dark web, where many payments are made in VA. • Prevalence of multistage predicate crime in the jurisdiction, e.g., human trafficking, investment fraud and romance/online relationship scams that involve investment in VA or payment in VA. • Consider the prevalence of the use of VA for criminal purposes. For VASPs • Countries can also refer to the sectoral vulnerabilities section of the ML NRA guidance, which states that the existence of unlicensed and/or unregulated sectors should be considered a factor in the vulnerability analysis, and that “off-the-books” informal businesses and services may be more prevalent in the VASP sector. Vulnerabilities should be considered also in relation to the features of the framework for the creation of legal entities or arrangements and their dissolution, e.g., speed of incorporation, inexpensive set-up of companies, limited requirements for incorporation and ability to incorporate using an international legal entity as sole shareholder/director. • Consider the prevalence of the misuse of VASPs for criminal purposes, including for ML. • Consider foreign threats as well, particularly if the country is an international financial centre. VA/VASP activities are cross border in nature and the risk of foreign VASPs operating in the jurisdiction should be analysed. • Countries should consider why VASPs are choosing to operate in their jurisdiction (e.g., no tax on VA, quick and easy to set up, innovation-positive economy), and if/how they are interacting with other service providers based or operating in the jurisdiction (e.g., payment service providers, banks). Countries should consider the risks of VASPs operating in the jurisdiction that may be using services outside of the jurisdiction (where there may be less regulation), which may increase the risk. • Regulatory arbitrage in the sector across different countries, when VASPs are incorporated in foreign jurisdictions with lax regulations, allowing them to operate and offer services globally without adhering to adequate AML/CFT compliance mechanisms.

Data sources	Data held on VA/VASP activity can vary significantly across countries. This is particularly the case where the VA/VASP sector is not regulated or has only recently become a reporting entity. Before beginning the risk assessment exercise, countries should first identify possible data and information sources about VA/VASPs, determine the gaps in their data and what other sources might be used to complement the data they collect. Countries can consider supplementing their existing data with other sources. This could include, but is not limited to: • NRAs of other countries and supranational risk assessments, if available. This could include risk assessments where VA/VASP links to the assessing jurisdiction or region have been noted. • National, regional and international studies on VA/VASPs produced by the public sector. Reports by international organisations (e.g., FATF, FSRBs, UNODC). • Industry engagement and feedback, e.g., through questionnaires, discussions, focus groups and direct engagement with the private sector, including VASPs. Discussions with subject matter experts, including academics conducting evidence-based research into ML risks. • Data from VASP supervisors, including levels of compliance with AML laws. If a VASP supervisor has not yet been assigned for AML/CFT, there may be other authorities involved in the regulation of VA activity who could provide information for the risk assessment. • Data from investment and capital market supervisors about the amount and types of investment products, brokerage and asset management activity known to involve some form of VA, whether as a direct product (i.e., initial coin offerings) or as a product in which the underlying value is set against a VA (e.g., stablecoins). • Informal international cooperation e.g., through questionnaires sent to key strategic partners about threats/vulnerabilities and possible links to the assessing country, and perceptions as to levels of ML risks linked to VA/VASP activity in the assessing country. Interpol and Egmont requests received and sent involving VA/VASP to gain insights into international investigations, intelligence sharing, and collaborative efforts to combat transnational organised crime and illicit financial flows. • Formal international cooperation, e.g., review of MLA requests received and sent involving VA/VASPs.[41] • Information and reports received by or produced by the FIU – Suspicious Activity Reports (SAR)/STR and other regular reporting, catalogue or list of VASPs operating in the country or region, vicinity if known, typologies and strategic analysis reports. • Requests for information received or sent under International Organisation of Securities Commissions (IOSCO) to financial supervisors, e.g., regarding alleged mis-selling by brokers operating in their jurisdictions. • Investigation data and cases handled by LEAs and the judiciary (e.g., case law) in which VA/VASP have been misused for criminal purposes, including to launder the proceeds of crime, to identify typologies. • Government statistics on the sector (e.g., from Ministry of Economy, Ministry of Trade), its size, growth and revenue generation relative to the national GDP, administrative tax cases brought before national tax authorities for non-declaration of assets or income linked to investment in or proceeds derived from the sale of VA. • Company or BO registry data concerning the number of legal persons identified as engaging in VA/VASP activity, the jurisdiction of residence

[41] 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 VASPs and credit card businesses. FATF (2024), FATF's Money Laundering National Risk Assessment Guidance,

	of those owning and controlling such entities and relevant financial information from annual accounts etc. • Consumer complaints received by supervisory authorities and law enforcement related to VA/VASP activity. • Open-source intelligence (OSINT) and information about VA/VASP activity in, from or linked to the jurisdiction such as accessibility of VA/VASP products to residents, annual flows of transfers or website activity in or from the assessing jurisdiction, reliable consumer websites reporting scams or unreliable VASPs linked to the country and blockchain analytics companies.[42] Information may also be available in forums, chats or messaging services. VASPs, including illegal VASPs, are likely to use the internet to advertise their services. As with all data, it is important to avoid bias and ensure that data comes from reliable and reputable sources. Countries that are not currently collecting their own data should consider doing so going forward, ensuring it is collected in such a way that it can be easily used during the risk assessment. This should include an ongoing evaluation of the data collected and the process for storing and updating it and a gap analysis to determine what data is missing and how it can be obtained.
Inclusion of private sector	Including the private sector in the VA/VASP risk assessment process is a good practice and can assist to both provide data where gaps exist and explain how specific VA/VASP products and services are used and misused. Country experience confirms that it is sometimes the most efficient way to get reliable information on risks. In jurisdictions where VA/VASP activity is prohibited or limited, banks and other FIs, such as e-payment, investment and money remittance businesses may have information on informal or illegal VA/VASP activities linked to the country.
Include red flag risk indicators	Red flag indicators which complement the country's risk assessment can help both authorities and the private sector to detect and report suspicious activity. The FATF's 2020 publication *Virtual Asset Red Flag Indicators of ML/terrorist financing (TF)*[43] may be referenced to complement the country's risk assessment and help authorities and private sector to detect suspicious activity. The FIU and VASP supervisor can further develop their own indicators that are present in the country, reviewing them regularly and updating as needed to incorporate emerging trends in this dynamic sector.
Impact on risk-based supervision	Any risk assessment that includes analysis of VA/VASPs should feed into the risk-based supervision of VASPs, including to inform the frequency and focus of on-site and off-site inspections.
Communication of the risk assessment findings	VASPs are the newest reporting entities to be brought under the FATF Standards, and therefore they may not be familiar with AML obligations and may struggle to understand outcomes of ML risk assessments. The communication of the results of the risk assessment should take this into account and frame the findings in the context of AML obligations for VASPs.

Box 4. VA/VASP risk assessment case studies

Luxembourg first integrated VAs as an emerging risk in its 2018 NRA on ML/TF and further recognised VAs and VASP as an emerging vulnerability in its 2020 NRA. Considering this, and in order to identify particular risks and design specific mitigation measures, the National Prevention Committee on ML/TF conducted a specific vertical ML/TF risk assessment on VAs and VASPs (VASP VRA) in 2020.[44]

[42] For example: TRM Labs, Chainalysis, Lukka, Elliptic, Merkle Science.

[43] FATF (2020), Virtual Asset Red Flag Indicators of ML/TF

[44] The Government of the Grand Duchy of Luxembourg (2020), *ML/TF Vertical Risk Assessment: VASPs,* Vertical Risk Assessment: Virtual Asset Service Providers. Section 3.2. Methodology provides a detailed description of the approach and methodology followed to assess the ML/TF risks of VAs and VASPs.

Luxembourg's VASP VRA defines VAs and VASPs, develops a comprehensive taxonomy of different types of VAs and VASPs, explains the main ML/TF threats they are exposed to in all stages of ML (i.e., placement, layering and integration), and describes the ecosystem services and key actors at every stage of the value chain (issuance, custody, exchange). To conduct the assessment, Luxembourg engaged with private sector representatives and academia through bilateral meetings, providing insights for both regulators and industry stakeholders.

The risk assessment analysed threats and vulnerabilities separately. The threat analysis examined the exposition to domestic and external predicate offenses as per the NRA that are more relevant to Luxembourg's VASP industry. With regard to the vulnerability assessment, it was conducted in two steps. First, the vulnerabilities assessment considered VA-specific factors that may lead a criminal to choose one type of VA over another for ML/TF purposes (anonymity, usability, security). Second, VASP-specific factors were assessed (market structure, ownership, products, geography, clients, transactions, and channels). The overall vulnerability score for VA (result of the first step) was integrated into the VASP assessment (second step) under the products and activities dimension, reflecting the risks associated with different VA offerings.

The VASPs VRA also dedicated a section to analyse how traditional finance may be exposed to VASPs ML/TF risks in Luxembourg. For instance, by being directly or indirectly being exposed to VAs, or by establishing VASPs as a separate/additional business. Finally, the VASPs VRA provided a list of legal obligations for the VASP private sector and presents a list of more than 40 red flag indicators developed jointly with Luxembourg's FIU that should specifically be considered in a VA context.

Source: Luxembourg

South Africa has maintained a vigilant stance on the ML/TF risks associated with VA, or crypto assets as they are known in South Africa. The 2018 ML NRA identified cybercrime and VA as high-risk areas. In response, South Africa conducted a dedicated "Crypto Asset and Crypto Asset Service Providers (CASPs) Risk Assessment" in 2020, highlighting the inherent vulnerabilities of VA to criminal abuse. The 2022 NRA expanded on this with a comprehensive chapter on VA and VASPs, analysing the sector's size, complexity, growth trends, and regional significance, noting that South Africa had the first VA exchange in Africa and plans to create the largest free-trade area in the world through the Africa Free Continental Trade agreement which would present new opportunities for the VA/VASP sector. It also included insights into VA adoption in emerging markets and regulatory gaps at the time, referencing FATF's 2020 VA Risk Indicators as well as the anticipated rise in use of VA for remittances and in developing countries and countries with volatile national currencies.

Following the inclusion of CASPs under AML/CFT regulation in December 2022, South Africa completed a new ML/TF risk assessment in 2025.[45] This assessment identified key red flags regarding methods used by criminals to exploit the vulnerabilities of the CASP sector, market drivers, and the inherent and residual

[45] Financial Intelligence Centre of South Africa (2025), *Assessment of the ML/TF Risks of CASPs*, 2025.3-PUB-Sector-risk-assessment-–-Crypto-asset-service-providers-1.pdf

risk factors for CASPs, their products, services, clients, transactions, delivery channels and geographical areas. It drew from wide consultation with public and private sectors (including regulators), comparative studies and regulatory reports filed by CASPs. As a result of strengthened mitigation measures—including new legislation, enhanced regulatory oversight, risk-based supervision, and administrative sanctions for non-compliance —the ML risk for CASPs has decreased from "high" to "medium-high." Continuous market monitoring and risk assessment support agile policy responses to emerging threats.

Source: South Africa

Egypt decided to prohibit VA/VASP on the basis of a preliminary risk assessment conducted in 2018. This was further supported by their 2023 VA/VASP risk assessment which identified several threats where VA/VASPs could be used misused for ML/TF. Egypt relied on sources such as cases from LEAs and public prosecution, STRs from FIs, open-source information, interviews (with academics, VA/VASP experts and private sector representatives), information from Blockchain analytics companies and international cooperation requests to draw its conclusions on the risks associated with VA/VASPs.

Noting that prohibition alone is not a "silver bullet" to preventing VA/VASP activity, Egypt has taken further actions to mitigate the risks. These include:

- Issuing guidance on seizure, confiscation and liquidation of VA and including training on the basics of VA within the training plans of LEAs and public prosecutors (e.g., how to identify VA wallets and QR codes during their investigations, identification of seed phrases, public and private keys and other issues related to VA).
- Issuing red flag indicators to FIs and fintech companies and giving training sessions to help them detect any VA activities
- Providing FIs with regularly updated lists of websites used in trading of VA and making them block and report transactions/attempted transactions with these websites
- Building public-private partnerships to introduce private sector technology and innovation in FIU operations
- Continuing to identify emerging risks of VA through analysis of VA transactions.
- Issuing warnings to the general public to raise awareness of the risks associated with VA.
- Creating a national VA wallet in order to seize VAs in violation of the Central Bank law no. 194 of 2020, which has resulted in an increase in, and facilitated recent successful asset seizures and confiscations.

Source: Egypt

Box 5. Legal persons and legal arrangements risk assessment statistics at a glance

- Assessing the risks of legal persons and arrangements is a challenge for many countries. Of the 60 countries that responded to the October 2023 survey for the ML NRA Guidance update project, 31 countries (55%) had conducted a risk assessment of legal persons within their NRA, and 19 (34%) had conducted a risk assessment of legal arrangements within their NRA.[46]
- Fifteen (27%) responding countries did a separate risk assessment on legal persons and/or legal arrangements.
- Mutual evaluation report (MER) and follow-up report (FUR) ratings for FATF members show that currently, 37% of countries have fully met criterion 24.2 on assessing the risks of legal persons and that 34% have only partly met or not met this criterion, showing that there is still work to be done in this area.
- Some common criticisms include a) inadequate scope and depth (e.g., incomplete coverage of all legal persons), b) risk assessments failed to address potential misuse of legal persons for criminal purpose, and c) overly domestic focus and lack of consideration of foreign legal persons or foreign ownership.

14. The 2013 FATF Methodology used in the previous round of mutual evaluations (i.e., for FATF, the 4th round of mutual evaluations) had different requirements to the 2022 Methodology.[47] The 2022 Methodology has new requirements for countries to assess the risks of legal arrangements and foreign-created legal persons and arrangements that have sufficient links with their country. These requirements will help countries develop a more complete picture of their risks.

15. This annex contains a quick reference guide table for assessing the risks of legal persons and legal arrangements, followed by some case examples from countries that have assessed the risks of legal persons and/or arrangements.

[46] Survey was in relation to the update of the ML NRA Guidance.

[47] The 2013 and 2022 FATF Methodologies can be found on the FATF Website: www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html.

Table 4. Considerations when assessing ML risks of legal persons and legal arrangements

To assess the ML risks of legal persons and legal arrangements, countries could consider the following:[48]

Consideration	Reasoning and comments
Analyse country risk and context	• Take into consideration relevant legal and regulatory contextual issues specific to the country, and the threats and vulnerabilities that country faces, e.g., PEP ownership of legal persons, foreign national ownership of legal persons. • Consider the country's attractiveness as a regional or international formation or incorporation center for non-residents, identify groups of non-resident clients for whom the jurisdiction is a preferred location for entity formation, and consider associated risks. Certain features that make a jurisdiction attractive for bona fide business investments (such as tax attractiveness, strong legal framework, economic stability, significant business sector of professional service providers catering to foreign clients) may also increase its attractiveness to illicit actors seeking to form legal entities or arrangements to hide or invest proceeds of crime. • Consider the legal framework of the country, for example, if trusts are not legally recognised, can foreign trusts still be legally administered by residents in the jurisdiction and if not, is there evidence that foreign trusts are being administered in the jurisdiction, nonetheless? It is important to look into the legal requirements to settle a legal entity or a trust, especially if it is mandatory to have information on the ownership, BO, entities in a group relationship, etc. • Is the country's definition of BO in line with the FATF definition of BO and what measures are in place for authorities to obtain both basic and BO information.
Process and drafting	Countries could consider including the following stakeholders: • Public sector: company registries, trust registries, FIUs, tax authorities, financial and non-financial supervisory authorities (especially Trust and Company Service Provider (TCSP) supervisors), judicial authorities, LEAs, anti-corruption agencies. • Private sector: company secretaries, law firms, TCSPs, business associations, civil society organisations and academics conducting evidence-based research into ML risks.
Conducting a mapping exercise of legal persons and legal arrangements[49]	Countries should complete a scoping exercise to identify all types of legal persons and arrangements created in the country, examining the different types, forms and basic features in order to analyse the risks. Identify and describe the processes for a) creating those legal persons; and b) obtaining and recording basic and BO information on those legal persons/arrangements.

[48] The suggested sources listed for data are non-exhaustive and should not replace data collection and analysis on a national level. Rather, the goal is to provide a variety of sources for background information that can support jurisdictions in the initial stages of research on their risks. It is recommended that countries assess the reliability of all sources used and do not take external data sources at face value, rather use them to supplement their national level data and risk understanding, especially where there are data gaps.

[49] FATF (2023), *Beneficial Ownership of Legal Persons*, paragraph 15-20.

The reference to "all" legal persons and arrangements includes those associations (for legal persons), trusts and/or foundations (for legal arrangements) that may be used for establishing an NPO. While countries may wish to examine the use of NPOs for fraud or ML, they should do so ensuring the assessment and any measures to safeguard the NPO sector are targeted and proportionate, and that governments do not enforce obligations regarding NPOs for ML purposes in a way that causes unintended consequences which are unduly disrupting or discouraging legitimate NPO activities.[50]

For foreign legal persons, the key element is identifying whether a legal person has "sufficient links" to the country. Countries can determine this on the basis of risk. This could include (but is not limited to) situations where the legal person:[51]

- Has a permanent establishment or branch or agency in the country, e.g., a foreign registered insurance firm sets up an agency office in the country to sell insurance products, but most of its financial operations are in a foreign jurisdiction.
- Has significant business activity in the country. Significant business activity may be defined either in terms of a monetary threshold, or by such other parameters as may be suitable to the particular situation of the country, e.g., a foreign incorporated trading company sources most of its raw ingredients from the country and has multiple long-term contracts with local suppliers.
- Has significant, ongoing business relations with FIs, VASPs or Designated Non-Financial Businesses and Professions (DNFBPs) subject to AML/CFT regulation in the country. Significance could be in relation to the size of the relevant market and/or the impact of the business activity in the relevant market or the areas/sectors in which a legal person operates, e.g., a foreign created investment firm with multiple business banks accounts with a bank based in the country to process international transactions, or a foreign real estate firm that relies on the services of lawyers and accountants in the country for property transactions.
- Has significant real estate or other investment in the country, including any asset subject to registration, such as ownership of high value commercial or residential real estate, securities market investment or other assets. Significant here could be determined with reference to the average price of the real estate/corresponding asset market in the country, or the quantity of real estate held, e.g., a foreign company with a portfolio of high-value properties in the country.
- Employs staff, or is a tax resident (i.e., by reason of having its place of effective management or administration there) in the country, e.g. a foreign-headquartered multinational company is legally incorporated in the country for tax purposes.

Countries should identify legal arrangements governed under national law, which are administered in their country or for which the trustee or equivalent resides in their country, and types of foreign legal arrangements that have sufficient links to the country. Countries could analyse types of legal arrangement individually as they may have different risk ratings, and different risk levels for ML and TF.

ML risks are commonly associated with the ways in which legal arrangements can represent obstacles to transparency.[52] Countries could consider the following:

- How different types of legal arrangements are recognised and defined in the laws of different countries.[53]

[50] FATF (2021), *Mitigating the Unintended Consequences of the FATF Standards*, (accessed 11 April 2025).

[51] See footnote 111 in the FATF Methodology (2022).

[52] FATF (2024), *Beneficial Ownership and Transparency of Legal Arrangements*, ,paragraph 49.

[53] See footnote 138 in the FATF Methodology (2022).

	• Legality of administering, managing or otherwise operating a legal arrangement established/ settled in a foreign jurisdiction.[54] • Nature of links identified between foreign legal arrangements and jurisdictions – country should identify and analyse the links and explain in the risk assessment which ones are deemed to have "sufficient links" to the country.[55] • Consider obstacles to transparency, e.g., private nature of arrangements, choice of law, ease of formation, flexibility, overlap of several parties to trust, flee clause, protection of assets, multiple layers and distance between beneficiary and other parties. Examples of foreign legal arrangements with "sufficient links" to the country can include but are not limited to:[56] • The trust or similar legal arrangement or a trustee or a person holding an equivalent position in a similar legal arrangement has significant and ongoing business relations with FIs, VASPs or DNFBPs in the country. Significant business could be in relation to the size of the relevant market and/or the impact of the business activity in the relevant market or the areas/sectors in which the trust or arrangement or a trustee or equivalent operate. • The trust or similar legal arrangement or a trustee or a person holding an equivalent position in a similar legal arrangement has significant real estate or other local investment in the country. Examples for such other local investment may include (but are not limited to) securities market investment. Significant real estate or other local investment could be determined with reference to the average price of the real estate and the corresponding asset market in the country, or the quantity of real estate held. • The trust or similar legal arrangement or a trustee or a person holding an equivalent position in a similar legal arrangement is subject to taxation in the country (e.g., VAT, income tax, property tax, wealth tax).
Data sources	Countries could consider the following data sources to support their risk assessment. This list in non-exhaustive.: • Analysing registration statistics on all types of legal persons and arrangements that can be created under their national laws, and the intended use of each type (e.g., tax vehicle, NPO, company).[57] The use of domestic legal persons in high-risk sectors or countries. • Examining the ease and speed at which a legal person or arrangement can begin to operate after being created, and if there are any supplementary requirements (e.g., having a bank account in the country, opening activities with the tax authorities). Analysing ease with which ownership of legal persons and beneficiaries of trusts can be changed and complex structures can be put in place. • Countries are encouraged to take a multi-agency approach to data gathering and obtaining case studies – including FIs, tax authorities and TCSPs. • Review and analyse SAR/STRs and cases or typology reports from LEAs and prosecutors in which domestic or foreign legal persons or arrangements have been misused for criminal purposes including ML. This can help identify common typologies for abuse. Countries should

[54] FATF (2024), *Beneficial Ownership and Transparency of Legal Arrangements*, paragraph 68.

[55] See footnote 142 to criterion 25.3(c) in FATF Methodology (2022) for explanation of "sufficient links".

[56] From FATF (2024), *Beneficial Ownership and Transparency of Legal Arrangements*, , paragraph 71.

[57] IMF (2022), *Unmasking Control: A Guide to Beneficial Ownership Transparency*, www.imf.org/en/Publications/Books/Issues/2022/10/06/Unmasking-Control-A-Guide-to-Beneficial-Ownership-Transparency-517096.

	record details on the nature of abuse, type of legal structure (e.g., with regard to nominee shareholders or directors and shell companies), jurisdiction of incorporation, concealment techniques in ownership/control arrangements, involvement of intermediaries (e.g., lawyers, accountants, TCSPs), and other details. • FIU statistics (e.g., on legal entities suspected of being abused for ML or predicate offences that are included in SARs/STRs reported to the FIU, analysed by the FIU or disseminated by FIU to LEAs). • Information gathered from FIs on dormant bank accounts linked to new entities with few transactions recorded. • Data from tax authorities on entities with no tax reports since they were created. Number of tax enforcement cases. • Data from tax authorities and FIs (cooperation between authorities required) on entities that have stopped submitting tax reports but still have bank account transactions. • Information on TCSPs including compliance records, data from supervisors etc. • Conduct expert consultations with external experts from the private sector, civil society, and academics conducting evidence-based research on ML risks, who hold expertise on setting up legal structures, on their benefits and risks. Review academic literature on legal persons and arrangements. • OECD's common reporting standard (CRS) reports[58] and Tax Information Exchange Agreements.[59] • Tax attractiveness index.[60] • Reports by international organisations highlighting typologies and risk indicators (e.g., FATF and Egmont's trade-based ML (TBML) risk indicators,[61] the FATF's report on Laundering the Proceeds of Corruption,[62] the World Bank's report on risks related to nominee services "Signatures for Sale"[63] and "The Puppet Masters" [64]). • Aggregate public procurement data - combined with tax information and financial intelligence - can be analysed for red flag indicators, e.g., the percentage of tenders awarded to legal persons created in the period just before tender announcements (a high percentage could suggest that tenders were prearranged), and links between procurement data with STRs filed and tax discrepancies (a red flag indicator would be companies that have not declared any revenue to the tax authorities being awarded contracts). Misuse of legal persons may be more common

[58] OECD, *Automatic Exchange Portal*, https://web-archive.oecd.org/tax/automatic-exchange/common-reporting-standard/index.htm (accessed 3 April 2025).

[59] OECD (2002), *Agreement on Exchange of Information in Tax Matters*, www.oecd.org/content/dam/oecd/en/publications/reports/2002/05/agreement-on-exchange-of-information-in-tax-matters_g1gh2b36/9789264034853-en.pdf (accessed 3 April 2025).

[60] Tax Attractiveness Index, www.tax-index.org/ (accessed 28 January 2025).

[61] FATF (2021), *Trade-Based ML Risk Indicators*,

[62] FATF (2011), *Laundering the Proceeds of Corruption*

[63] World Bank (2022), *Signatures for Sale: How Nominee Services for Shell Companies are Abused to Conceal Beneficial Owners*, https://star.worldbank.org/publications/signatures-sale-how-nominee-services-shell-companies-are-abused-conceal-beneficial

[64] World Bank (2011), *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It*, https://openknowledge.worldbank.org/entities/publication/ec364fd2-92f8-58a0-bd4e-155ac0f644d6

in certain sectors than others, so countries can consider whether there are differences in sectoral vulnerabilities.

- Incoming and outgoing MLA and other international cooperation requests related to legal persons and legal arrangements.
- Objective press reports and independent, investigative journalism can provide useful background information and context.[65]
- Information from academics, interviews with subject matter experts and NPOs conducting evidence-based research into ML.
- Countries can supplement their knowledge through the analysis of cross-border risks, international cooperation, typologies report, etc.

For domestic legal persons specifically:[66]

- Collect and analyse registration statistics (e.g., incorporation volumes and trends) on all types of legal persons that can be created under their national laws.
- Investigate advertising practices by TCSPs promoting the jurisdiction as an international centre for incorporation/entity formation to non-residents - which attributes (e.g., anonymity, asset protection) are they advertising to non-residents to attract incorporation business?

For foreign legal persons specifically:[67]

- Cross-border transaction monitoring from FIU can show where funds have been moved between multiple legal persons in different jurisdictions (especially high-risk jurisdictions and tax havens) and show links with foreign legal persons.
- Countries should consider their jurisdiction's exposure to risks stemming from legal persons created in high-risk jurisdictions subject to a call for action or under increased monitoring of the FATF, or jurisdictions subject to economic or financial sanctions, embargoes or similar measures that are related to TF and issued by organisations such as the UN.

For legal arrangements specifically:

- Data on creation and registration of legal arrangements (e.g. quantity of legal arrangements created, their nature etc.) from corporate or trust registries (where applicable) or tax authorities.
- Cross-border transactions monitoring from the FIU involving trusts.
- Records of investments linked to trusts (BO registry) e.g., real estate, luxury goods, companies. Records of trusts that hold bank accounts and other assets.

[65] Countries are encouraged to have multiple independent sources, ensure not to use media funded by special interest groups or biased reports from nationally controlled media.

[66] FATF (2023), *Beneficial Ownership of Legal Persons*, paragraph 18.

[67] Ibid. Paragraph 16-19.

Box 6. Legal persons and legal arrangements risk assessment case studies

New Zealand included a full chapter in its 2024 NRA on legal persons and legal arrangements.[68] This chapter looks closely at the risk and context of New Zealand and analyses the vulnerabilities of these structures. The assessment identifies key factors of risk, such as the ease of creating legal persons in New Zealand, and the use of nominee directors to obscure BO. New Zealand's reputation as a politically and economically stable jurisdiction further increases the perceived legitimacy of legal persons, which can make them more appealing for transnational criminals looking to hide illicit funds.

The NRA also explores the role of TCSPs in facilitating the misuse of legal persons and arrangements, as they may provide nominee director services, registered addresses for a company (known as virtual offices) and legal structures that span multiple jurisdictions, which introduces challenges in identifying and preventing illicit activities.

New Zealand has included several case studies to show how legal persons and legal arrangements have been exploited in practice, for example to launder the proceeds of fraud, drug trafficking and other transnational crimes. A table of the top ten jurisdictions from which persons are connected to foreign trusts is also included.

Source: New Zealand

China conducted a risk assessment on legal persons using the World Bank Tool, covering both domestic and foreign legal persons with significant links to China. The assessment involved on-site visits, expert interviews, and data collection from authorities, FIs, DNFBPs and the general public via questionnaires.

China performed both qualitative and quantitative analyses on the data and information, including a review of over 30 000 ML cases involving legal persons. The assessment examined threats by crime type, legal person type, region and sector. Inherent risks were evaluated based on factors such as entity size, ease and cost of formation and attractiveness to non-residents while residual risks were evaluated based on registration conditions, information disclosure requirements and enforcement measures.

Findings showed legal persons are frequently misused for fraud, illegal fundraising, corruption, illegal gambling, and tax evasion—aligning with NRA results and expert input. In response, China established a central BO registry using a risk-based approach (simplified for low-risk entities and enhanced for high-risk entities), improved legislation to enhance BO verification by FIs and impose stricter requirements for higher-risk entities and formed a multi-agency task force to tackle shell company misuse.

Source: China

Türkiye conducts a separate risk analysis of legal persons, which is also used as an input in the country's NRA for both its vulnerability and consequence analysis. Türkiye's legal persons assessment also includes a separate assessment of companies operating in Türkiye that are limited taxpayers or have more than 50%

[68] New Zealand Police FIU (2024), *New Zealand NRA 2024 on ML/TF/PF*, www.interest.co.nz/sites/default/files/2025-03/fiu-nra-2024.pdf.

foreign partners. As a non-trust law country, Türkiye addresses risks from potential trust-like arrangements within this analysis and provided guidance and awareness on foreign trusts. The first assessment was conducted in 2021 and updated in 2025.The methodology categorises risk under five factors for both domestic and foreign companies in addition to consideration of purchase of real estate by foreign companies.

1. Cash transactions and money transfers (e.g., the company does not have any credit transaction; high number and value of Turkish Lira/foreign currency cash transactions in the accounts of the Company or its shareholders (last five years) that may not be commercially related in a way that causes suspicion of ML/TF abuse).
2. Misuse of point-of-sale (POS) devices and credit cards (e.g., although the person with the registered POS device is a partner, representative or authorised representative of the company, the financial profile of this person is not suitable for this as it poses a risk of ML/TF).
3. BO transparency (e.g., multiple companies with same representative, STRs, being sanctioned for non or incorrect reporting to the BO registry, frequent changes of BO information in the registry).
4. Suspected forgery in domestic trade (e.g., a company that consistently announces losses continues to operate in a way that is likely to create the impression of ML/TF abuse, intensive purchase and sale of goods in a way that exceeds its economic capacity, operating with inadequate number of personnel, historical records on tax evasion).
5. Suspected forgery in foreign trade (e.g., commercial or customs documents supporting that transactions are incomplete, appear forged, contain incorrect or misleading information, intensive export or import transactions contrary to the ordinary course of commercial life of a company, STRs).

ML/TF scenarios and red flags serve as proxy indicators linked to these risk factors. Risk scores are assigned to companies, and average scores are calculated by company type and sector. Concentration of risk per company type and sector are then estimated based on deviations from these averages.

The analysis uses data from the FIU, Revenue Administration, Ministry of Trade, BO Registry, and other sources including criminal records, banking data, and sanction lists. Results are shared with relevant stakeholders.

Source: Türkiye

Nigeria undertook a thematic inherent and residual risk assessment to evaluate the misuse of legal persons and legal arrangements in mainland and free trade zones.[69] The exercise drew participation from authorities including the Central

[69] NRA Forum of Nigeria (2022), *National Inherent Risk Assessment of Legal Persons and Legal Arrangements in Nigeria*, https://nigsac.gov.ng/niradocs/Legal%20Persons%20%20Legal%20Arrangements%20NIRA%20report_Oct2022_01.pdf

Bank of Nigeria, Corporate Affairs Commission, Nigeria Export Processing Zones Authority, Oil & Gas Free Zones Authority and the Nigerian FIU.

The assessment considered the various types of legal persons and arrangements and the registration processes by the relevant company registries. It then analysed their vulnerabilities and risk levels based on ownership structure, expert opinion, governance and oversight structure, STR analysis, and usage for criminal activity.

Analysis of international intelligence reports from foreign jurisdictions, showing that Nigerian citizens (including PEPs) had used foreign trusts to hide illegally acquired assets. Legal arrangements are not commonly used in Nigeria, but the risk assessment identified them as a significant vulnerability for ML. By leveraging international intelligence and real-world cases, Nigeria was able to see that Nigerian actors have been involved in schemes abusing legal arrangements abroad. The findings of the report helped the competent authorities implement appropriate mitigating measures including setting up a national BO Registry with a discrepancy reporting feature and ensure authorities in certain areas identified as in need of special attention, developed regulation for BO disclosure (e.g., for companies operating in Free Zones).

Source: Nigeria

Jordan produced an ML/TF risk assessment focused on legal persons and legal arrangements in 2023.[70] The risk assessment contains a detailed description of the types of legal persons and arrangements that exist in Jordan and are within the scope of the risk assessment. The assessment looks at BO, which is important given the context of the country. The assessment considers existing risk mitigation measures concerning the legal requirements for transfer of BO, requirements on checks and balances in the governance of legal persons and arrangements, and the availability of BO information, which allows an evaluation of threats, vulnerabilities and residual risk.

The risk assessment includes calculations of the percentage of foreign BO of legal persons, and whether they have "high risk" nationality (based on the FATF list of high-risk jurisdictions and other sources) or are from a country that faced or is still facing conflicts and unstable conditions. This was then used to adjust the risk rating.

Jordan provided risk ratings for all types of legal persons and arrangements present in the country and gave separate ratings for ML and TF given the different risk levels identified. The risk matrix that is detailed at the end of the risk assessment shows how the various elements evaluated have combined to give the risk ratings.

Source: Jordan

[70] Jordanian authorities (2023), *Money Laundering and Terrorist Financing Risk Assessment of Legal Persons and Legal Arrangements in Jordan*, www.amlu.gov.jo/EBV4.0/Root_Storage/EN/EB_HomePage/Money_Laundering_and_Terrorist_Financing_Risk_Assessment_of_Legal_Persons_and_Legal_Arrangements_in_Jordan.pdf

Box 7. Informal economy statistics at a glance

- Levels of informality vary among countries. More than 60% of the world's employed population, that is two billion people, earn their livelihoods in the informal economy. The emergence of non-standard forms of employment, including through the rise in digital labour platforms, is also pushing the boundaries of the informal economy around the globe.[71]
- An estimated 1.4 billion adults worldwide are unbanked. The majority of unbanked adults worldwide are women (women 13% unbanked vs. men 11% unbanked).[72]
- The World Bank's Prospects Group has constructed a global database of informal economic activity including up to 196 economies over the period 1990-2020. Self-employment and informal employment in either the formal or informal sector are among the most commonly used measures of informal economy.[73]
- Several MERs refer to "informal economy", "shadow economy", "aquarium economy" and the use of cash[74] and informal financial services or underground banking either as important contextual factors or a vulnerability that require action by countries in terms of better understanding and/or addressing the problem.[75] This factor/vulnerability also features in some country NRAs.
- Some of the factors that determine the size of a country's shadow economy are bureaucratic quality, corruption control and GDP per capita.[76]

[71] UN Development Programme, *Informal Economy Data Explorer*, https://data.undp.org/insights/informal-economy (accessed 20 March 2025).

[72] World Bank, *Financial Inclusion Overview*, www.worldbank.org/en/topic/financialinclusion/overview#:~:text=The%20expansion%20of%20digital%20financial,owning%20an%20account%20by%202021 (accessed 15 May 2025).

[73] Elgin, C., M. A. Kose, F. Ohnsorge, and S. Yu. (2021), *Understanding Informality*. CERP Discussion Paper 16497, Centre for Economic Policy Research, London. www.worldbank.org/en/research/brief/informal-economy-database

[74] It is important not to confuse cash usage for illegitimate reasons (e.g. tax avoidance, ML) with general cash usage. Access to cash is also important from a financial inclusion perspective especially for vulnerable categories of people such as the elderly, uneducated and people with disabilities. See: FATF (2025), *Financial Inclusion and AML/CFT Measures*, Guidance-Financial-Inclusion-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf, footnote 99.

[75] For example, Nicaragua's MER notes over 75% of transactions occur in the informal economy and queries impact on overall system (e.g. application of CDD in financial and non-financial designated entities). Italy's NRA describes the informal economy as a vulnerability of the socio-economic system. The MER notes the high use of cash and relatively large informal economy very significantly increases the risk that illicit proceeds may be rechannelled into the regulated formal economy.

[76] The Association of Chartered Certified Accountants (2017), *Emerging from the shadows, the shadow economy to 2025*,

16. Informality makes it easier for criminals to operate, both for committing a predicate offence and for laundering the proceeds. It is therefore an important contextual factor and a potential vulnerability that can be exploited. Where relevant to their risk and context, countries should focus on the effects of the prevalence of the informal economy to their AML system, the size of the economy, cash activities and the prevalence of informal financial services. Analysis of the informal economy could be incorporated into the analysis of different threats and vulnerabilities in the NRA, since it can often be a cross-cutting issue, rather than as a stand-alone chapter.

17. Countries can have many reasons for assessing their level of informal economy including for policy making and taxation, including the development of risk-based AML/CFT policies including simplified measures for assessed lower risk areas. This means that some authorities involved in this exercise may not be directly part of the AML/CFT regime. This presents an opportunity for domestic co-ordination with, for example, the national statistics office of the country or whichever authority is responsible for compiling statistics about population, income, commerce, etc. and to leverage their work.

18. Assessing and understanding the level of financial exclusion and inclusion in a country is key to for understanding the ML risks related to the informal economy. Financial exclusion may arise from multiple factors that limit access to and usage of formal financial services, and can be an unintended consequence of inappropriate or insufficient application of the risk-based approach to ML, TF and PF risks. Financial exclusion not only harms individuals and businesses but can also represent a real risk to achieving effective implementation of FATF Standards by driving financial activity into unregulated channels.[77]

19. To consider the relevant ML risks the analysis of the informal sector should cover its root causes and the interplay between financial exclusion, the informal economy, and informal service providers. The risks of financial exclusion are mitigated through financial inclusion measures that increase reliance on regulated, registered or licensed financial services, ultimately strengthening the integrity of the financial system. NRAs should also consider a country's success and effectiveness in reducing the informal economy and use of informal service providers, as a risk mitigating measure. Countries should also consider the impact of government initiatives to cut informality and increase financial inclusion (e.g., simplified measures for assessed lower-risk scenarios),[78] as having more transactions and activity taking place in the formal financial system can help to mitigate some risks. Crucially, when considering the risks represented by products, channels or initiatives seeking to bring formerly informal activity into the formal financial system, countries should compare these with the risk represented by leaving the same activity in the informal economy, and not with an imaginary baseline in which the activity does not take place at all.

www.accaglobal.com/content/dam/ACCA_Global/Technical/Future/pi-shadow-economy.pdf (accessed 20 March 2025).

[77] FATF (2025), *Financial Inclusion and AML/CFT Measures*, Guidance-Financial-Inclusion - Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf, paragraph 25.

[78] For more details and examples of simplified measures and efforts to increase financial inclusion, countries are invited to consult FATF (2025), *Financial Inclusion and AML/CFT Measures*, Guidance-Financial-Inclusion-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf

20. As already noted in the NRA guidance, the private sector also has a key role by identifying unlicensed, unregistered financial service providers. These unlicensed, unregistered competitors put them at a disadvantage due to the lack of regulatory burden.

21. Useful working definitions to reflect on in this section:

- **Informal economy**: As defined by the OECD.[79] Also characterised by the absence of regulation of economic and commercial activity and the frequent use of cash which is apparent or normal to the population.[80] In an AML context, this makes FIs and DNFBPs less susceptible to report transactions involving large amounts of cash. The size of the informal economy is often measured using domestic or international labour statistics.[81] It is important to note that informal economy is not only about informal businesses - it also includes off-the-record transactions of legitimate businesses.
- **Shadow economy:** Refers to people who either operate entirely outside the tax and regulatory system or are known to the authorities, but do not correctly report their tax obligations.[82] Another definition is that it refers to market-based production of goods and services whether legal or illegal that escapes detection in the official estimates of GDP.[83] May be used interchangeably with "informal economy".
- **Use of cash or cash economy:** Focuses on the use of cash for high value transactions, cash-intensive lines of business such as trade in vehicles and works of art, and more broadly preferred over other payment methods.[84]
- **Informal financial services providers**: Entities that offer financial services without regulatory oversight or supervision. These providers operate outside formal financial systems and often rely on personal relationships and community trust. High levels of use of informal financial services may point to financial exclusion from formal financial services and can be addressed by effective financial inclusion policies.

[79] OECD (2002), *Measuring the Non-Observed Economy – A Handbook*, www.oecd.org/en/publications/measuring-the-non-observed-economy-a-handbook_9789264175358-en.html.

[80] GAFILAT (2015), *Regional ML Threat assessment*, https://biblioteca.gafilat.org/wp-content/uploads/2024/04/AnalysisRegionalThreatsGAFILAT.pdf.

[81] ILO, www.ilo.org/ilo-employment-policy-job-creation-livelihoods-department/branches/employment-investments-branch/informal-economy (accessed 15 May 2025).

[82] The Treasury of Australia's definition of the shadow economy, available here: https://treasury.gov.au/policy-topics/economy/shadow-economy (accessed 15 May 2025)

[83] IMF (2000), *Shadow economies Around the World Size, Causes and Consequences*, available at: www.imf.org/external/pubs/ft/wp/2000/wp0026.pdf, page 4 (accessed 14 January 2025).

[84] Brazil (2021), *NRA Executive Summary*, www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/avaliacao-nacional-de-riscos/4-1_executive-summary_national-risk-assessment_ing.pdf page 14 (accessed 14 January 2025), Germany (2019), *First NRA*, www.bundesfinanzministerium.de/Content/EN/Standardartikel/Press_Room/Publications/Brochures/2020-02-13-first-national-risk-assessment_2018-2019.pdf?__blob=publicationFile&v=9 page 99 (accessed 14 January 2025).

- **De-risking:** The phenomenon of FIs refusing to provide, terminating or restricting business relationships with categories of customers (or individual customers) in order to avoid risks altogether, rather than sufficiently understanding and managing the risks in line with the FATF's risk-based approach.[85]

22. As noted in the NRA Guidance, 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 in a foreign jurisdiction. While informal usually means something that is "in the shadows" and difficult to measure, there are indicators and assumptions that countries have used to measure informal economy and its impact on criminality including ML.[86]

Table 5. Considerations for ML risk assessment of the informal economy

Countries could consider, but are not limited to, the following:[87]

Consideration	Reasoning and comments
Analyse country risk and context	• Take into consideration relevant legal and regulatory and contextual issues specific to the country, and the particular threats and vulnerabilities the country faces in terms of informal economy, use of cash, cash economy or shadow economy (see definitions above). • The informal economy may be assessed as one of the contextual factors that can impact risk levels by facilitating certain threats (e.g., fraud) and risks (e.g., use of cash and informal transfer methods). • Analyse the size and nature of the informal economy in the country, including whether it is focused on particular regions or populations. For example, some countries find it useful to measure the difference in between household consumption and disposable income considering all known sources of income and assuming that difference is in the realm of the grey/black economy. Looking at estimated returns in certain sectors and the level of credit afforded to that sector to operate has also been considered. Countries have also looked at detected crimes as a source to calculate the black economy or sources of illegal informal income assuming this only represents 10% of what total estimates could be.[88] • Analyse how the prevalence of the informal economy is impacting the implementation of AML controls by the private sector, (e.g., STRs not being filed by actors in the informal economy) and examine how this

[85] FATF (2025), *Financial Inclusion and AML/CFT Measures*, Guidance-Financial-Inclusion - Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf, paragraph 47.

[86] The ILO provides data points to be collected in its Recommendation 204: https://normlex.ilo.org/dyn/nrmlx_en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:R204 (accessed 15 May 2025).

[87] The suggested sources listed for data are non-exhaustive and should not replace data collection and analysis on a national level. Rather, the goal is to provide a variety of sources for background information that can support jurisdictions in the initial stages of research on their risks. It is recommended that countries assess the reliability of all sources used and do not take external data sources at face value, rather use them to supplement their national level data and risk understanding, especially where there are data gaps.

[88] Braho A. (2017), *Assessment on the extent of Informal Economy in Kosovo*, Study funded by the EU in the framework of Project "Further support to Kosovo Institutions in the fight against Organised Crime, Corruption and Violent Extremism".

	impacts the level of risk. • Analyse how the prevalence of the informal economy is impacted by the design of the AML controls by the private sector, e.g., derisking or financial exclusion due to inappropriate identity verification requirements. • Analyse the main drivers of the informal economy (e.g., cultural habits, tax concerns or lack of trust in formal entities). • Consider the level of financial exclusion and any national or regional level initiatives to increase financial inclusion. Lack of financial inclusion pushes individuals and businesses toward informal economic activities. For example, if an individual is not able to open a bank account due to lack of sufficient identification, they may be forced to rely on cash transactions, which are outside of the formal financial system and cannot be tracked.
Process and drafting	Countries could consider including the following stakeholders: • Public sector: Ministries of Labour and employment, trade union associations, FIUs, customs authorities, immigration authorities, LEAs, security and intelligence agencies and local government authorities. • Private sector: market associations, microfinance institutions, mobile money operators, trade associations, remittance service providers and civil society organisations.
Data sources	Countries could consider the following data sources to support their risk assessment. This list is non-exhaustive.: • Value of small remittances by domestic workers vs. transactions occurring in unlicensed financial services where large amounts of funds are moved. Small domestic remittances may be done through mobile money or wallet to wallet transfers. • Frequency and volume of cash transactions, ratio of cash transactions to total transactions, Currency in circulation and cash to GDP ratio. • Avenues to consider when assessing use of cash include which channels are predominantly used to launder domestically (e.g., purchase of vehicles or art) and how much cash goes outside country borders. • Cash transaction reports by FIs and DNFBPs if required by the country and received by the FIU can be useful statistics to create a heatmap of cash use. • Information from LEAs on investigations and prosecutions related to the value of the cash proceeds of corruption or tax offences. • Reports by other international organisations (e.g., International Labour Organisation (ILO), International Monetary Fund (IMF), World Bank, OECD) on the informal economy, use of cash, statistics on how informality facilitates crime and ML in the jurisdiction. • Central Bank or other statistics on unlicensed or unregistered activity, statistics on money aggregates. • National and International statistics and research on financial inclusion and financial exclusion, such as the World Bank's Findex database.[89] • Engagement with micro-lending entities which often deal with informal businesses and promote financial inclusion. • Collaboration between banks and tax authorities to analyse statistics on credit granted, revenues and tax declarations.

[89] World Bank, Global Financial Inclusion (Global Findex) Database, https://microdata.worldbank.org/index.php/catalog/global-findex/?page=1&ps=15&repo=global-findex (accessed 19 May 2025)

	• Supervisory actions against unlicensed or unregistered entities. • Engagement with private sector on estimated unlicensed or unregistered financial or non-financial activity. • Tax authority data on audit, fiscalisation, tax collection. Data on cases of tax evasion.

Box 8. Informal economy risk assessment case studies

China leverages its economic data system to assess the scale and impact of the informal economy in its national risk assessment. To measure the informal economy, China uses several information sources:

- Registration and statistical authorities estimate the number of registered and unregistered businesses. China's statistical department conducts a national economic census every five years. Through indicators such as "whether registered" and "whether paying value-added tax/income tax" the number of informal economic entities can be screened out. The proportion of registered to unregistered businesses is estimated using cross-verification and data sharing with the tax authorities and social security. The authorities also perform daily regulatory inspections of market activities.
- Tax authorities match registered businesses with tax records to identify those operating informally.
- Financial regulatory authorities, including the People's Bank of China analyse data from FIs and trends in private lending to estimate the scale and proportion of transactions not included in the formal financial system.

To mitigate risks, China's market regulatory authorities conduct targeted operations against unlicensed businesses while promoting financial inclusion, guiding businesses to engage in economic activities in compliance with the law through standardised administrative processes and regulatory innovation. Regional efforts include:

- Shanxi Province conducts inspections and targeted risk assessments to identify and map out unlicensed businesses.
- Yumen City has designated commercial streets, school vicinities, urban-rural junctions, and commodity trading markets as priorities for enforcements, as well as industries that pose public health risks.
- Xi'an City combines guidance and enforcement, adjusting actions based on the severity and intent of violations.

Source: China

Indonesia's rapidly growing e-commerce sector has significantly contributed to its economy, with transaction values increasing from IDR 106 trillion (approximately USD 7.8 billion) in 2018 to IDR 266 trillion (approximately USD 19.1 billion) in 2020.[90] However, this expansion has also led to concerns about the informal economy and its implications for tax evasion and ML.

[90] Exchange rates have been taken from 1 January 2018 and 1 January 2020 respectively.

The 2021 Annual Report of the Central Bank found that a key issue is the lack of transparency in business ownership, as many merchants receiving funds from major e-commerce platforms are registered under the names of family members or employees rather than the actual business owners. This opacity allows businesses to underreport income, avoiding tax obligations and potentially facilitating illicit financial flows. Furthermore, a study of nearly 800 000 merchants found that 81.4% lacked a Taxpayer Identification Number, raising concerns about tax evasion and unregulated financial activities. The estimated tax loss from merchants exceeding IDR 4.8 billion (approximately USD 3.4 million) in transactions annually amounts to IDR 108.7 billion (approximately USD 7.7 million), with additional potential tax liabilities of IDR 3.1 trillion (approximately USD 220 million).[91]

Indonesia noted the need to balance the rapid growth of the sector, which contributes positively to its economy, with developing effective oversight mechanisms to mitigate potential risks of misuse by criminals, enforcement of business ethics, and the potential for state losses due to the loss of tax revenue in the shadow economy. Some of the risk mitigating measures introduced include Know Your Merchant (KYM) provisions for e-commerce and online marketplace platforms and more detailed KYM requirements for business-to-business (B2B) e-commerce platforms and the introduction of regulations for e-commerce platforms to increase tax obligations. In 2024, Indonesia assessed the risks and impact of the shadow economy in the natural resources sector, expanding the methodology to the mining, palm oil plantation and forestry sectors. The risks considered were related to legal activities taking place in these sectors including such as tax avoidance and unrecorded activity related to trade finance, as well as illegal activities. These sectors were considered the highest risk due to the use of cash transactions to avoid tax obligations and hide the proceeds of unauthorised plantation activities.

Source: Indonesia

The use of cash is identified in Israel and around the world as a significant element in the creation of a "black market economy", the existence of which perpetuates the discrepancy between reported economic activity and true economic activity, tax evasion, money laundering and the financing of organised crime. A governmental committee established in September 2013 including the main competent authorities for AML examined the risks resulting from the use of cash and other untraceable methods of payment. The committee recommended an action plan and possible measures of implementing a strategy for restricting the use of cash to reduce economic crime and ML.

Israel combines multiple data sources in its data collection for NRAs. Comparing and analysing cash transaction reports and STRs with international wire transfer reports and trade statistics related to a counterpart country can reveal inconsistencies and anomalies that may indicate potential ML activities. For instance, if intensive cash transactions are observed, alongside high-volume international transfers where the counterpart country is known for very limited

[91] Exchange rates have been taken from 1 January 2021.

trade with the country, this discrepancy may suggest illicit financial flows and warrant further investigation.

Source: Israel

Annex B: Cross-comparison of Money Laundering threats and categorisation of threats and vulnerabilities

23. The purpose of the annex is to provide countries with a cross-country aggregation of risk information to highlight possible areas of focus, e.g., which predicate offences and which types of ML are most common on a domestic and international level, and how countries may wish to prioritise analysis of the associated risks. Countries should note that some areas of focus, predicate offences or types of ML that are included here will not apply equally to all countries. The purpose of the annex is to offer ideas on how to get started with this type of analysis, based on a variety of available sources.

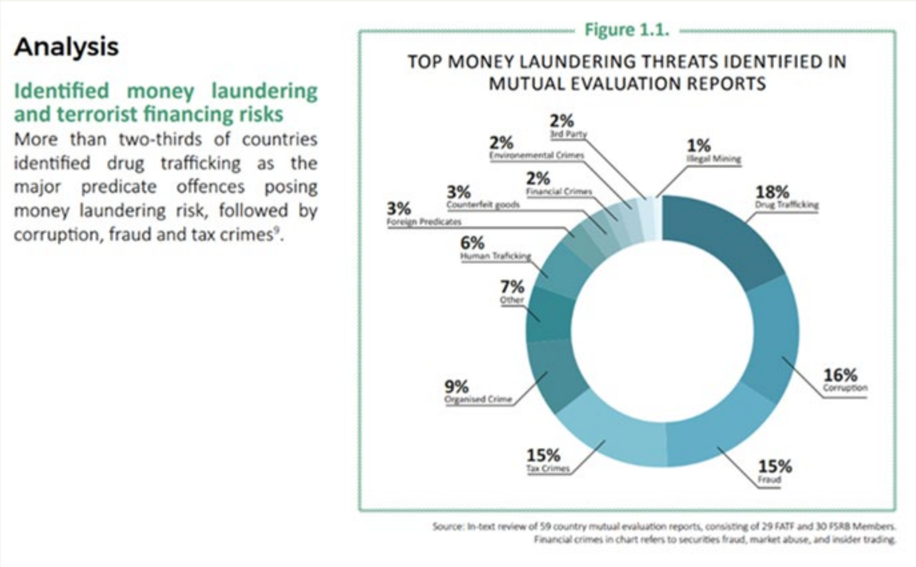
24. While the basis of every risk assessment undertaken by a country should be its specific and unique risk and context, countries may wish to consider the below information as a tool to kick-off or supplement their risk assessment and support prioritisation of certain common predicate offences. This annex is not intended to replace the country's own analysis of its risks, but consideration of commonalities present in their region or on an international level may provide a broader picture of the risk landscape. This is particularly important due to the cross-border nature of ML, which is constantly evolving with advances in technologies.

Major predicate offences according to MER analysis

Box 9. Statistics on ML threats

Figure 1. Top ML threats identified in MERs

This figure shows the top ML threats identified from country MERs. It is based on FATF Secretariat analysis of a sample of 59 country MERs from across the Global Network. All threats countries noted were domestic, apart from the category of "foreign predicates". However, foreign predicates may be under-reported, as subsequent questionnaires sent to the Global Network for the ML NRA Guidance update project showed that many countries face challenges effectively assessing the risks associated with foreign predicate offences.



Analysis

Identified money laundering and terrorist financing risks

More than two-thirds of countries identified drug trafficking as the major predicate offences posing money laundering risk, followed by corruption, fraud and tax crimes[9].

Figure 1.1.

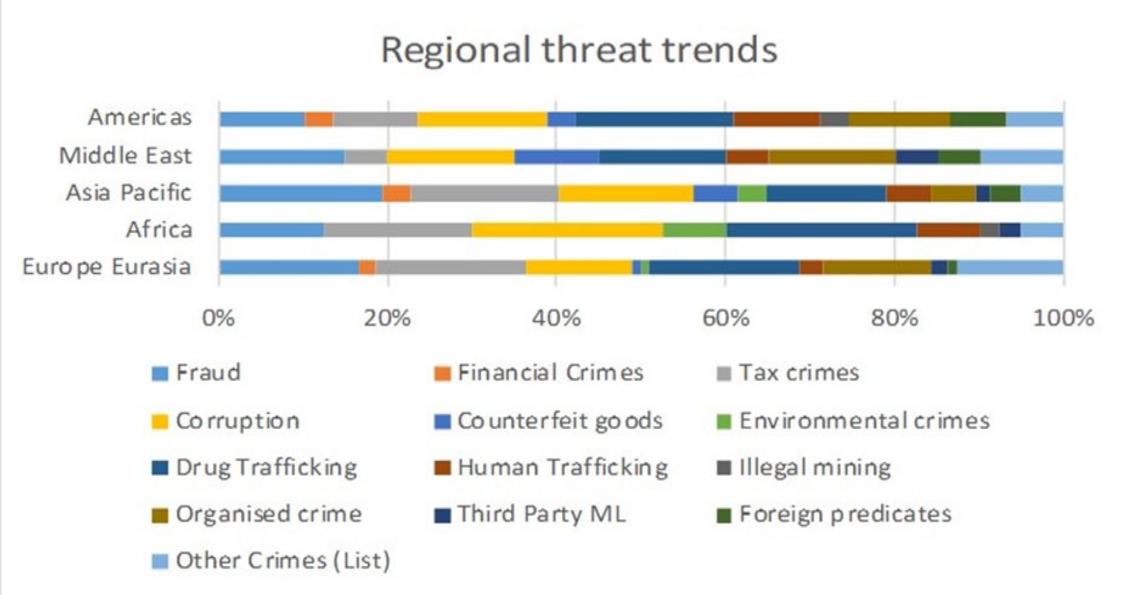
TOP MONEY LAUNDERING THREATS IDENTIFIED IN MUTUAL EVALUATION REPORTS

Source: In-text review of 59 country mutual evaluation reports, consisting of 29 FATF and 30 FSRB Members. Financial crimes in chart refers to securities fraud, market abuse, and insider trading.

Source: FATF Report on the State of Effectiveness and Compliance with the FATF Standards, 2022

Figure 2. Regional threat trends

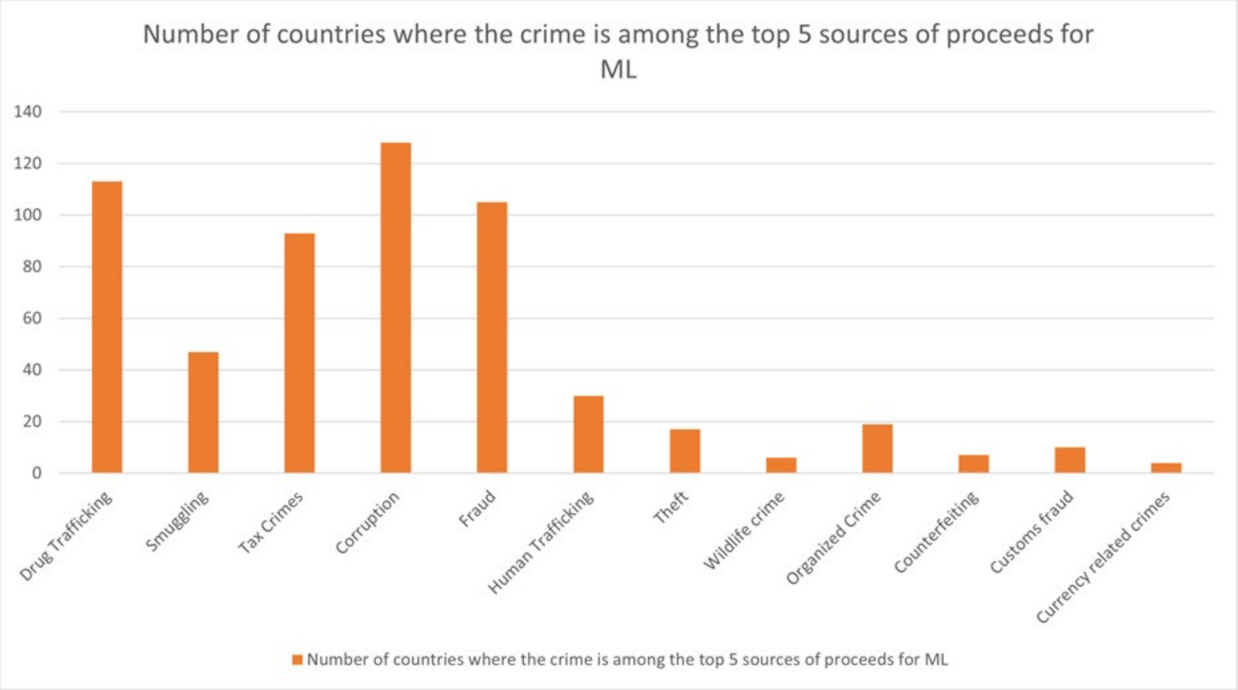
This figure shows regional trends in the top ML threats identified from country MERs. It is based on FATF Secretariat analysis of a sample of 59 country MERs from across the Global Network.



Source: Internal research by FATF Secretariat. Data collected for the FATF Report on the State of Effectiveness and Compliance with the FATF Standards, 2022.

Figure 3. World Bank analysis of top ML threats

This figure shows the top ML threats based on World Bank analysis of 147 MERs from across the Global Network.



Source: Unpublished Research by World Bank, 2022

25. Additionally, countries may wish to consider including in their NRA an analysis of why particular threats (e.g., those that are most prevalent on an international and especially regional level and involve cross-border elements) are *not* assessed to be material in the country. Including this information, together with the sources analysed to come to this conclusion, can increase transparency and support the continuity of the NRA process, and can facilitate the reassessment of threats on a longer-term basis. Countries are encouraged to liaise within their FSRB, with other regional bodies, and with neighbouring countries to broaden their risk understanding beyond their borders, which is especially important for many ML risks that involve cross-border elements at different stages of the ML process. All these suggestions are subject to the prioritisation and availability of resources, noting resources available to conduct assessments might be limited and should be used in the most efficient manner. Risk assessments should also be kept manageable and of a reasonable length to remain accessible and useful to both the government and the private sector.

Major predicate offences according to proceeds of crime estimates

26. It is worth noting that the estimates of proceeds of crime give a different ranking to the analysis in the previous section based on what were considered the highest risks in country MERs.

27. The following table provides information on major predicate offences (i.e., those frequently identified in MERs) ordered based on estimated proceeds of crime. The estimates in this section have been taken from various reliable sources and are

based on different methodologies. The estimates in this section are not considered to be definitive given the difficulties acknowledged in estimating proceeds of crime, the difference in methodologies used and that some of the estimates may already be (or later become) outdated. They are presented here for illustrative purposes, to encourage countries to consider the importance of predicate offences on an international level, even if they are not of high importance in the country itself. Countries may look for updated estimates from reliable sources when they come to update their NRA or prioritise other risk assessment work, and in many cases also do their own estimations.

Table 6. Annual global estimates of proceeds of predicate offences to ML

Predicate offence	Estimated annual proceeds (USD)
Fraud	5.38 trillion[92]
Corruption and bribery	3.6 trillion[93]
Drug trafficking	1.6 trillion[94]
Counterfeiting currency, counterfeiting and piracy of products	1.13 trillion[95]
Tax crimes	483 billion[96]
Environmental crime: Illegal logging Illegal mining Illicit waste trafficking	110-281 billion[97]: 10-15 billion[98] 12-48 billion[99] 10-12 billion[100]
Human trafficking	236 billion[101]

[92] Crowe and University of Portsmouth (2021), *The Financial Cost of Fraud 2021*, https://f.datasrvr.com/fr1/521/90994/0031_Financial_Cost_of_Fraud_2021_v5.pdf (accessed 30 January 2025) .

[93] UN (2018), *The costs of corruption: values, economic development under assault, trillions lost, says Guterres*, https://news.un.org/en/story/2018/12/1027971 (accessed 30 January 2025) .

[94] UNODC (2011), *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*, www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf (consulted 30 January 2025) .

[95] Global Financial Integrity (2017), *Transnational Crime and the Developing World*, https://gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final.pdf (accessed 30 January 2025) .

[96] EU Tax Observatory (2021), *The State of Tax Justice 2021*, www.taxobservatory.eu/repository/the-state-of-tax-justice-2021/ (accessed 30 January 2025).

[97] RHIPTO, INTERPOL and GI (2018), *World Atlas of Illicit Flows*, https://globalinitiative.net/wp-content/uploads/2018/09/Atlas-Illicit-Flows-FINAL-WEB-VERSION-copia-compressed.pdf. This figure includes proceeds for: forestry crime, illegal mining, waste trafficking, the illegal wildlife trade, illegal extraction and theft of oil, and crimes associated with illegal fishing. (accessed 15 May 2025) .

[98] World Bank (2012), *"Dirty Money" in Illegal Logging Can be Tracked and Confiscated, says World Bank Reports*, www.worldbank.org/en/news/press-release/2012/03/20/dirty-money-illegal-logging-can-tracked-confiscated-world-bank-reports (consulted 14 March 2025) .

[99] FATF (2021), *Money Laundering from Environmental Crime*,

[100] FATF (2021), *Money Laundering from Environmental Crime*,.

[101] International Labour Organisation (2024), *Annual profits from forced labour amount to US$ 236 billion, ILO report finds*, www.ilo.org/resource/news/annual-profits-forced-labour-amount-us-236-billion-ilo-report-finds (consulted 14 March 2025).

28. The "top four" predicate offences are often cited as being fraud, corruption, drug trafficking and tax crimes. As all these crimes could have cross-border elements, it is recommended that countries consider the risks of proceeds of these crimes entering their jurisdictions for laundering, even if the offence is not prevalent domestically.

Risk analysis of threats incorporating the consequences of crime

29. As outlined in the FATF's 2024 ML NRA Guidance,[102] countries should analyse the likely consequences of ML and predicate offences. The FATF defines risk as a threat taking advantage of a vulnerability to produce a consequence. Depending on the risk and context of the country, some predicate offences with a higher human, societal or environmental cost may need to be prioritised in the NRA to better understand threats and develop proportionate risk-mitigating measures.

30. The disparity in the placement of fraud and drug trafficking above may indicate that countries facing significant levels of these offences are rightly including other considerations such as the damage caused by drug trafficking on both individuals and societies. This may lead to it being considered a higher risk in many countries, despite generating fewer proceeds than other predicate offences. Other predicate offences (e.g., human trafficking and sexual exploitation) also threaten social stability and national security. They can cause strain on the resources of LEAs, weakening their effectiveness and creating vulnerabilities that could be exploited by criminals.

31. Corruption in particular can be pervasive in a variety of sectors, e.g., infrastructure, health, customs, tax, law enforcement, the judiciary, and natural resource management. This can lead to serious consequences on the population, for example, barriers to accessing basic healthcare, education and justice, or public safety risks such as the endangerment of human life due to unsafe infrastructure or lack of medicine.

32. As mentioned in the ML NRA Guidance, it is also important to consider the cross-border consequences of ML. When ML is international, 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.[103]

33. Considering both financial and social harm in the NRA can help countries better prioritise criminal threats, ensuring that both the financial system and broader society are protected from illicit activities. Giving greater focus to certain offences that may represent less financial profit but greater, long-lasting, or life-threatening effects does not mean deviating from also pursuing those major predicates which represent massive financial loss. It serves to ensure that authorities responsible for AML do not ignore or sideline certain crimes that generate fewer proceeds and lose opportunities to pursue crime with high societal impact.

34. Countries will however need to develop a yardstick to be applied consistently to ensure that the NRA informs a proportionate, risk-based approach. To ensure an efficient allocation of resources across the AML regime, as envisaged in Recommendation 1, the NRA needs to distinguish between higher and lower risk. The

[102] FATF (2024), ML NRA Guidance

[103] Ibid. page 34.

likelihood and extent of the activity and the consequences can help inform conclusions about their relative severity and importance.

Types of Money Laundering

35. The Report on the State of Effectiveness and Compliance with the FATF Standards[104] found that in the study of 59 MERs from across the Global Network, ML investigations and prosecutions were most likely to concern cases of self-laundering, or non-complex ML schemes (as opposed to complex ML schemes which are known to cause the greatest harm to society). The report also showed that IO.7 is one of the lowest rated Immediate Outcomes, with 99% of FSRB members rated low or moderately effective, implying that only 1% were effectively prosecuting and convicting ML cases. Among FATF members, two thirds were rated low or moderately effective. Eighty-two percent of countries across the global network were not prosecuting ML activity in line with their risks, according to their MER, and less than a third of the countries reviewed that were effective (Substantial or High effectiveness ratings) in IO.1 were pursuing investigations and prosecutions in line with their risks.[105]

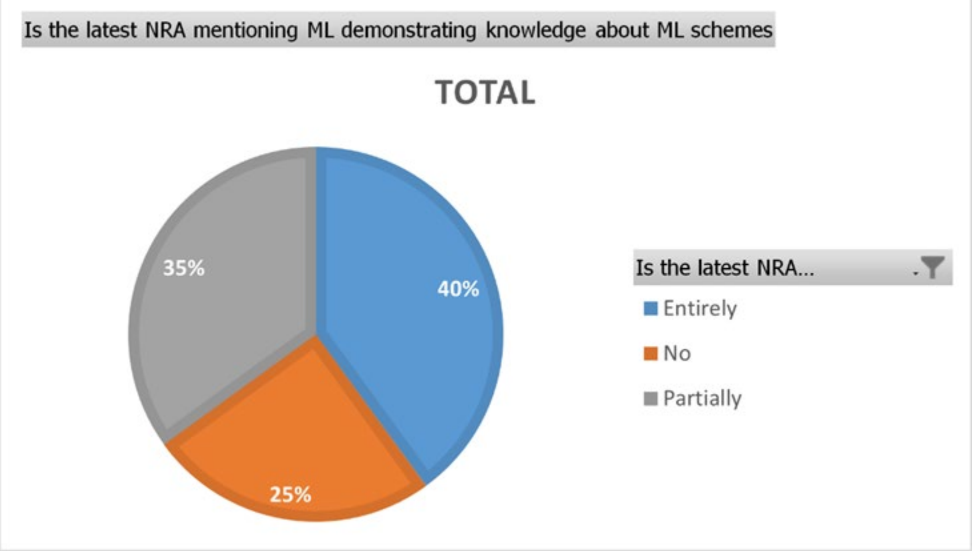
36. Further analysis undertaken by the FATF Secretariat of 40 NRAs (from countries that made the full version of the latest NRA available, i.e., not just the executive summary or risk ratings) from across the Global Network studied the extent to which countries demonstrate knowledge about different types of ML in their NRA.

[104] FATF (2022), Report on the State of Effectiveness and Compliance with the FATF Standards, Chapter 6.

[105] Information taken from a FATF Secretariat study of 59 MERs.

Box 10. Analysis of knowledge of ML schemes outlined in the NRA

Figure 4. Graph showing percentage of countries that demonstrated knowledge of different types of ML schemes in their latest NRA

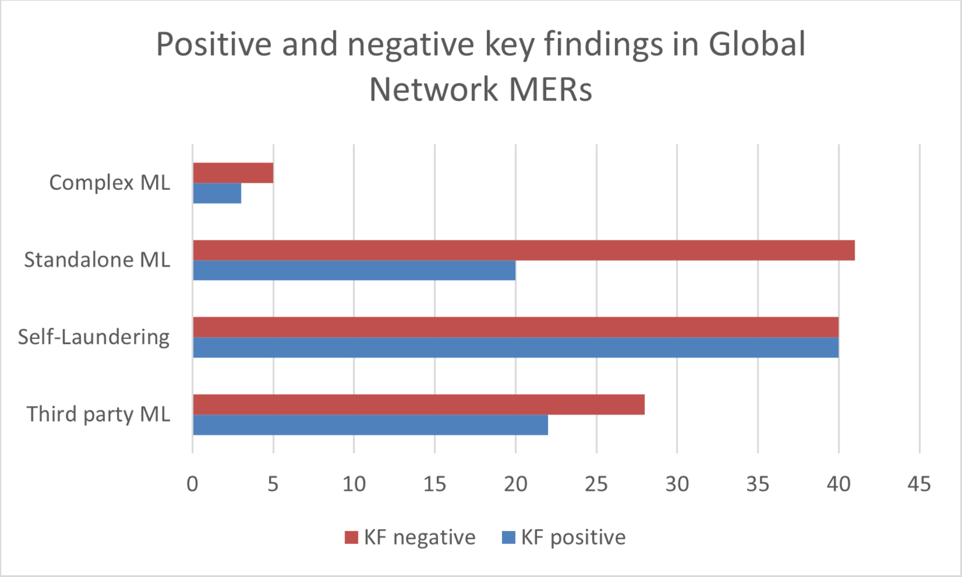


Note: The sample used was 40 NRAs from across the Global Network, where the full document was made available to the Secretariat. Therefore, it may not be fully representative of the Global Network as a whole, and is presented here for illustrative purposes.
Source: Unpublished research by the FATF Secretariat

It was found that 40% of countries (16 out of 40) demonstrated a detailed knowledge, that is to say that those NRAs highlighted multiple cases of ML, both simple and complex (e.g., with cross-border elements) that the jurisdiction identified and prosecuted. The explanations given were concise and showed that these countries had a good understanding of complex ML schemes and how they may be structured.

Thirty-five percent (14 out of 40) provided some ML cases, but these were generally simple ML schemes with few actors involved, or limited in quantity and lacking precision, with very limited discussion of complex cases. Twenty-five percent (10 out of 40) were found to have no case studies or explanations of complex cases (i.e., no concrete examples of third-party ML or cross-border ML), and limited examples of simple cases. A reason for this may be that the country had not identified any complex cases in their jurisdiction at the time of the NRA.

Figure 5. Positive and Negative Key Findings in Global Network MERs



Note: The sample used was 187 MERs from across the Global Network.[106]
Source: Unpublished research by the FATF Secretariat

The different types of ML are often referenced in key findings of MERs, often under IO.7 which deals with the investigation and prosecution of ML. The graph above shows the number of times the type of ML is referenced in a positive light (e.g., the country is investigating and prosecuting a type of ML in line with its risks) or in a negative light (e.g., that the country is focusing all its efforts on one type of ML and neglecting the others).

37. The limited exploration of different types of ML in NRAs including how it intersects with different threats and vulnerabilities in countries may in part explain the findings of the Report on the State of Effectiveness and Compliance with the FATF Standards. If a country does not assess and understand its risks, it is unlikely to demonstrate effectiveness in prioritising investigations and prosecutions for ML in line with its risk profile.

38. Giving focus to how ML takes place in practice, regardless of the predicate offence that generated the funds, can bridge the gap between predicate offences and laundering techniques. It is of course important to know which predicate offences are most common in the country, as this can support the prioritisation of law enforcement efforts to reduce crime. Knowing the vulnerabilities can help governments introduce or strengthen measures to address weaknesses. But examining the modus operandi shows how the illicit funds move in practice, and highlights the tools and channels exploited. It is also an effective way of keeping track of developments in ML

[106] While efforts were made to ensure comprehensive coverage, variations in terminology across MERs mean that some relevant references may not have been captured by the search terms used, or instances may have been double counted in some cases. As a result, there may be some omissions or duplications in the dataset and therefore it is presented for illustrative purposes.

typologies, for example as criminals adapt to new technologies, or find new ways to circumvent risk mitigating measures. It can also help countries target the mitigating measures introduced, for example if a specific product is being exploited to launder money, measures could address this specifically rather than an entire sector. Matching threats and vulnerabilities with the techniques used to launder money can help countries develop a more comprehensive understanding of the risk landscape and where the highest risks are concentrated.

Box 11. Focus on types of ML in the risk assessment

Germany's NRA spans over a number of individual publications providing in-depth analysis for the financial sector and non-financial sectors and techniques (e.g., legal persons and legal arrangements, financial agents and VA), within which a differentiation is made according to the type of ML.

The approach does not primarily focus on predicate offenses of ML. Germany's penal code includes all crimes as potential predicate offenses for ML, and so illicit proceeds can come from all criminal offenses from all over the world. However, selected, particularly relevant predicate offenses are evaluated more closely, including studies with regard to which generate the most proceeds of crime.

Germany's approach involves identifying modus operandi in detail as well as the circumstances and reasons why the perpetrator may have chosen this modus operandi. Vulnerabilities in the AML system are also taken into account and an assessment is made as to how likely it is that this mode will be used for ML in Germany. Finally, Germany looks at the extent of the presumed or actual impact and damage caused. Where available, quantitative data (e.g., evaluations of SARs and transparency register data) were used as a basis for each step of the analysis. This was supplemented with qualitative experience and expert opinion from the NRA working group, among other sources.

Source: Germany

Categorising factors of ML threats

39. The following is a list of threat categories that may be useful in building a picture or estimate of ML threats. This list is not exhaustive, and the individual categories should be viewed as examples and may be complemented in accordance with the purpose and scope of the assessment. It should therefore not be treated as a checklist to be completed for every risk assessment, but a pool of factors that countries can examine to increase risk understanding.

40. Threat factors that can impact ML risk relate to the prevalence and nature of domestic and foreign predicate offences and ML, including cross-border elements, the sectors, technologies and channels that are exploited, the perpetrators involved and inherent features that increase a country's exposure to crime.

41. By categorising threats, countries can gain a deeper understanding of the various factors that contribute to the risk landscape of the country. Countries should consider threats at all three stages of ML: placement, layering and integration.

Table 7. Threat categorisation

Threat factor	Categorisation elements
Direction of illicit funds for ML	• This analysis can include whether the illicit funds are mainly: ○ Domestic (funds originate in the country and are laundered in the country) ○ Inward (funds originate outside the country and are laundered in the country) ○ Outward (funds originate in the country and are laundered outside the country) ○ Transit (funds originate and are laundered outside the country and country is used for transit/layering).
Predicate offences,[107] considering factors such as:	• Prevalence of the overall crime in the country ○ Estimated size of proceeds generated ○ Proportion of ML investigations that involve the predicate offence • Prevalence of crimes in neighbouring countries or the region more generally, including ○ Nature and extent of relevant predicate offences ○ Amounts of proceeds of crime generated abroad and laundered domestically[108] ○ Cross-border in and outflows of proceeds of crime/ laundering offshore and foreign predicate crime • Regional and international situation • Sources, location, and concentration of criminal activity, including within underground areas in the economy • Which predicate offences that generate proceeds for ML occur in the country, in foreign jurisdictions, in both the country and foreign jurisdictions, and where the origin of the funds is not known.
Sectors, sub-sectors, products and services exploited, considering factors such as:	• Prevalence (in terms of case quantity, size of proceeds, etc.) of ML exploiting the sector • At what stage(s) of ML is the sector exploited • Any specific ways the sector is being exploited to launder illicit proceeds, including to facilitate the transit of illicit funds from/to foreign jurisdictions • Whether the sector has entities that operate regionally or internationally
Perpetrators, considering factors such as:	• Adherence to crime groups, their international / regional connection • Number of perpetrators arrested, prosecuted and convicted • The role of various perpetrators (e.g., mastermind, money mule) ○ age, occupation, income, nationality

[107] See the definition of “designated categories of offences” in the Glossary of the FATF Methodology

[108] It is difficult to calculate the proceeds generated from crime and then laundered, especially in cases where perpetrators have not been caught and assets have not been recovered. There is no established best practice to do so. Countries could consider the following: amount of illicit funds mentioned in court reports, information from STRs, general crime statistics to extrapolate data (i.e., have certain predicate offences increased or decreased over the years?). The OECD has provided guidance on identifying and quantifying proceeds of bribery: *Identification and Quantification of the Proceeds of Bribery*.

	○ methods of recruitment ○ PEP status • Characteristics of ML: stand alone, third parties, legal persons • Modus operandi
Typologies and techniques for exploitation	• TBML (through over and under-invoicing, etc.) • Service-based money laundering (through over- and under-invoicing etc.) • Exploitation of VA/VASPs (by using mixers, transferring VA using unregulated VASPs, etc.) • Abuse of legal persons and arrangements (e.g., by exploiting corporate accounts or change of directorship of companies.) • Professional money launderers • Money mules • Properties, jewellery, luxury goods, antiques, luxury vehicles, auctioned goods, virtual gold.
Technologies exploited	Note: some of these technologies may be used in such a way that a country becomes a transit point for illicit funds. This is possible due to the speed of online transactions and potential to obfuscate the source of funds, the originator and the beneficiary. • Cross-border payment gateway • Inter-bank payment system • AI: used to generate fake identification information to bypass KYC requirements and AI-assisted fraud to create fake accounts (e.g., money mule accounts) • Use of virtual private networks (VPN), proxy servers and misleading websites for conducting financial transactions. • Mobile banking. • Use of Social Media tools like running misleading ads on platforms like X (formerly Twitter), Facebook etc. to reach out to unsuspecting new customers in other jurisdictions. • Use of "groups" on encrypted messaging services like Telegram to reach out to unsuspecting individuals in other jurisdictions. • Use of VA
Other channels exploited, such as:	• Cash smuggling • Automated Teller Machines (ATMs) • Gift cards • Resident/non-resident legal persons • Credit/debit card lending
Inherent exposure to crime based on environmental and contextual factors	• Countries with abundant scarce natural resources • Countries with porous borders • Countries situated in major drug production areas or trafficking routes • Countries with financial centres and trade hubs.

Contextual factors and ML vulnerabilities

42. Identifying relevant vulnerabilities is key to developing a country's understanding of its ML risks. This list contains examples of contextual factors that may be considered at this stage of the ML risk assessment to help identify relevant vulnerabilities. They have been generally arranged according to the analytical framework known as "PESTEL" (an acronym based on the first letters of the major categories: political, economic, social, technological, environmental and legislative). This list is neither exhaustive nor binding, nor would these factors apply in every country's ML NRA and they should be applied in the context of each country (i.e., those that are "relevant" to the country).

43. Contextual factors may impact a country's vulnerabilities. Vulnerabilities can exist on a national or sectoral level. A brief explanation of how these factors can impact ML vulnerabilities has also been included.

Table 8. National level contextual factors and vulnerabilities

Contextual factor	Categorisation elements	Linked vulnerabilities, exacerbating factors and explanations
Political factors	• Structure of the political system. • Stability of the present government. • Level of political commitment and prioritisation of AML programmes. • Level of political commitment to fighting crime. • Commitment to undertaking or reviewing NRA in a timely manner. • Government reach in all areas of the country. • Adequacy of human, financial, and other resources of competent authorities – e.g., lack of specialised training, technological capabilities. • Levels of corruption; existence of investigations or prosecution of known corruption cases.	• Political factors can impact the strength of oversight and enforcement of AML laws and regulations. This can make a country attractive for criminals, including money launderers, and facilitate their illicit activities, including cross-border ML. • Other aspects to consider regarding competent authorities in general: ○ AML programmes are not prioritised and risk mitigation measures are not put in place or are not implemented effectively. ○ Risk understanding is not up to date among competent authorities meaning risk-mitigating measures and prioritisation of resources may not be appropriate. ○ Regulatory powers are insufficient to allow national competent authorities to address the issues on identification and verification beneficial owners of foundations, associations and other similar entities, such as trusts, legal persons and arrangements more vulnerable to abuse for ML. ○ Low or no engagement with private sector about regulatory expectations for compliance with national AML requirements, typologies or emerging ML risks or expected application of controls to mitigate ML risks. ○ Poor co-ordination and information-sharing among national authorities including law enforcement and intelligence agencies involved in

	• Effectiveness of engagement of private sector with AML obligations. • Effectiveness of operations of competent authorities.	combating ML, leading to inconsistent or conflicting processes and prioritisation among competent authorities responsible for combating ML. ○ Weak inter-agency cooperation in AML processes and operations. ○ Weaknesses in the authorities' ability to gather and share information due to a lack of capacity or legal privilege. ○ Lack of overall AML oversight by authorities. ○ Lack of international and regional engagement on AML issues, including on requests for assistance. • FIU ○ Decrease in the FIU's capability to process STRs received and develop typologies. • LEAs ○ Failure of LEAs to use analysis of STR data to initiate and prioritise ML investigations, both domestic and cross-border. ○ Decrease in capabilities of LEAs to suppress ML (e.g., inability to detect and investigate ML). The impression that particular predicate offences are not prioritised for investigation and prosecution, and there are no consequences to committing crime. ○ Poor conversion rates of STRs into ML investigations and prosecution of predicate offences to ML. Conversion rates of ML prosecutions and predicate offence convictions, asset seizure and forfeiture orders. ○ Systemic weaknesses in law enforcement, and in authorities' efforts to counter crime generally, in particular ML. ○ Lack of ability of intelligence and LEAs engaged in combating ML to use financial information in their investigations. • Customs ○ Borders, especially porous borders, can be exploited for ML. ○ No/weak cash courier control at border points. ○ Low conversion rates from customs inspections to seizures and prosecutions. ○ Lack of access for border and immigration officials to INTERPOL I-

		24/7 global police communication system. • Supervisors o Weak oversight or supervision and sanctioning of FI and DNFBPs. • Private sector o Risk understanding is not up to date among private sector, meaning risk-mitigating measures and prioritisation of resources may not be appropriate. o Requirements of AML regime not well understood or implemented by FIs, DNFBPs and VASPs allowing illicit funds to enter the financial system, low levels of compliance by private sector or specific sectors, with national AML requirements such as conducting risk assessments and quality of STRs. o Better AML awareness in FIs, DNFBPs and VASPs and stronger civil society engagement help mitigate ML vulnerabilities by increasing understanding of institutions role in AML and detecting illicit activity.
Economic factors	• The type of economic system. • The effectiveness of regulation within the economy. • Average earnings of the population (countries may calculate this differently depending on their specific context). • Currency exchange regime and rates. • Cost of public services and cost of living. • Size of the financial services industry. • Level of transparency of the financial system.[109] • Ownership/ control of FIs and requirements	• Factors such as the openness, size and complexity of the financial sector can impact vulnerabilities, especially when there is low regulation, as there are more avenues for ML abuse. • Ineffective regulation introduces gaps or loopholes that can be exploited by criminals. • Economic disparity among the population can increase the likelihood of use of informal transactions and activities related to corruption. • Countries with large informal sectors and cash-intensive economies may be at higher risk of ML as many transactions take place outside of the formal financial system and cannot be tracked. Exploitation of weak application of controls by illicit actors in relation to the use of cash to purchase real estate/ luxury goods. • The cost of services in the formal financial system may exclude certain populations from access and push them to informal systems. • Exploitation of loopholes or exemptions under legislation permitting non-residents to misuse domestic legal persons through concealment of their

[109] IMF, *Central Bank Transparency code,* www.imf.org/external/datamapper/CBT/browse/ (accessed 15 May 2025).

	concerning the identification of beneficial owners that are non-residents. • Corporate governance arrangements in FIs, VASPs and DNFBPs. • Nature and role of legal persons and legal arrangements in the economy. • Nature of payment systems and the prevalence of cash-based transactions. • Acceptance by VASPs of cash transfers for conversion to VA. • Cash-based economy with large informal sector; percentage of cash outside legitimate banking system, especially relative to comparable countries.[110] • Application of FI secrecy and other secrecy –including professional secrecy. • Geographical spread of financial industry's operations and customers. • Alignment of AML obligations or control measures of countries with FATF Recommendations.	identity. • Poor corporate governance practices of reporting entities may be linked to ML cases or reported activity. • VA/VASPs have been known to be exploited for ML purposes. Given the lack of consistency in regulations worldwide, criminals may target jurisdictions with weak regulation for ML. • Vulnerabilities linked to low effectiveness of FIs, DNFBPs and VASPs in implementing AML obligations or control measures, such as: ○ Customer due diligence ○ Ongoing due diligence, including transaction monitoring ○ Reporting measures currently performed ○ Internal controls ○ Record-keeping
	• The demographics of the society • Extent of social	• Certain demographics be more vulnerable to cyber-enabled fraud and scams. Some reasons include the increase in digitalisation of payments, increase in engagement with the online space in general since the COVID pandemic including those that are less tech-

[110] IMF (2023), *Measurement and Use of Cash by Half the World's Population*, www.elibrary.imf.org/view/journals/001/2023/062/article-A001-en.xml

	inclusiveness[111] • Significant population shifts – e.g., increasingly aging population, levels of migration or emigration. • Cultural factors, and the nature of civil society • Areas of social, ethnic or political conflict • Literacy level and extent of awareness of citizen rights among the populace. • Financial literacy and financial inclusion programmes • Level of derisking in the country	savvy.[112] • Social exclusion and financial illiteracy increase reliance on informal networks, raising ML risks due to lack of traceability. It can also increase the vulnerability of populations to criminal activity such as human trafficking and participation in organised crime groups. • Conflict and political instability create opportunities for illicit financial flows due to lower regulation and oversight of financial activity. • High cultural reliance on cash transactions and informal finance makes ML harder to detect due to lack of transparency of transactions.
Technological factors	• Use of transportation • New communication methods e.g., social media and messaging services. • The use of technology in money transfer and introduction and use of new payment methods • Use of AI in cases where there is no face-to-face contact. • Deepfakes	• Technological advancements impact how ML occurs and how authorities can combat it. Criminals are quick to adapt new technologies, so having an updated understanding of risk is important. Lack of regulation, or recent regulation in new technologies can mean gaps exist which criminals can exploit. • Many technologies allow for instant, anonymous international transfer of funds which are hard to trace. • Methods of transporting cash across borders and how this is detected, how TBML occurs may change with adoption of new technologies, abuse of emerging transportation technologies such as automated systems and methods of obscuring vessel ownership can also lead to ML vulnerabilities. • New communication methods such as social media and messaging apps can be exploited to commit crimes such as fraud.

[111] There are World Bank and UN tools to help measure this: World Bank, *The Social Inclusion Assessment Tool*, https://pubdocs.worldbank.org/en/478071540591164260/siat-logo-web.pdf, and UN (2010), *Analysing and Measuring Social Inclusion in a Global Context*, www.un.org/esa/socdev/publications/measuring-social-inclusion.pdf (consulted 21 March 2025)

[112] For example see reports by OCCRP (2021), *Report: Minorities and Women are More Likely Victims of Cyber Crime*, www.occrp.org/en/news/report-minorities-and-women-are-more-likely-victims-of-cyber-crime and FATF (2023), *Illicit Financial Flows from Cyber-Enabled Fraud*, Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

		Encrypted information sharing channels can enable coordination amongst criminal groups. • New payment methods through digital payment services providers – services that are provided by non-bank PSPs may be more vulnerable to abuse for ML as they may fall outside of the AML regime. • AI and deepfakes could be used to circumvent KYC requirements and ongoing CDD leaving the financial sector vulnerable.
Environmental factors	• Global environmental factors such as availability of water, global warming, and other climate-related issues. • Impact of the local environment on crime such as housing, security etc. • Impact of environmental legislation. • Compliance with environmental restoration obligations.	• Natural disasters and resource scarcity can see an increase in predicate offences such as corruption, fraud and environmental crimes such as illegal logging and waste trafficking. • Weak or unenforced environmental laws and regulations can facilitate illegal resource extraction. Lack of transparency in industries can also increase ML risks. • Funds allocated to environmental restoration may be misappropriated.
Legislative factors	• Criminal justice system and legal environment • Ease with which new legislation can be passed • Review process for current legislation • Impact of international standards on national legislation • Strengths and weaknesses in legislation combating serious and organized crime • Strengths and weaknesses in current AML legislation	• Weak criminal justice systems allow criminals to evade prosecution. This can give the impression that there are no consequences to crime and allow criminals to re-offend. • Delays in the legislative process or lack of regular review of legislation can slow down the adoption of AML measures leaving laws and regulations outdated and open to exploitation by criminals. • Vulnerabilities arising from weaknesses in legislation combating serious and organised crime. • Vulnerabilities arising from weaknesses in current AML legislation, like: ○ AML preventive controls, including AML specific supervision and monitoring, that collectively do not deter ML nor result in it being detected if it does occur. ○ Lack of AML cross-border controls and international cooperation. ○ Jurisdiction not a party to the UN Convention against Transnational Organised Crime (UNTOC) and its

		Protocols, and/or the UNCAC. ○ Lack of adherence to international standards or conventions applicable to the specific sector or product. ○ ML not criminalised or inadequately criminalised, standalone ML not criminalised, incomplete coverage of predicate offences to ML. ○ Financial sector not prohibited from conducting relationships with shell banks or shell companies. ○ Inadequacy of AML controls, in areas of customer due diligence, ongoing due diligence including transaction monitoring, reporting measures currently performed, internal controls, record keeping, lack of regulation on BO. ○ Lack of guidance to relevant authorities on BO. ○ Limited or absence of risk-based approach guidance on AML provided by regulatory, oversight and supervisory authorities. ○ Limited regulation of money or value transfer systems. ○ Entities not registered and size of sector unknown. ○ No system of registering or licensing service providers; difficult to take enforcement action and thereby to formalise flows of funds. ○ Any non-AML controls that apply to entities that can be abused for ML, including general supervision or monitoring. ○ Inefficacy or inadequacy of non-AML related cross-border controls, including general border security. ○ Ineffective or inadequate compliance audits. ○ Rules or guidance not enforced. ○ Lack of a regulator or supervisors. ○ Legal or other constraints on products, services, transactions. ○ Coverage of requirements in other countries for entities operating in more than one jurisdiction.

Table 9. Sectoral-level vulnerabilities

Vulnerability factor	Categorisation elements
By sectors, such as:	• Banks and other FIs (as outlined in the FATF Standards), which may include sub-categories like: o Securities o Insurance o Money services businesses o Other FIs • VASPs • DNFBPs (as outlined in the FATF Standards) • Other entities that do not fall under the FATF definition of FI, DNFBP or VASP may also be considered depending on the risk and context of the country, for example: o Advisors, including tax and financial o Bookmakers, betting, gaming & lotteries o Motor vehicle retailers o Boat charterers, sellers, and re-sellers o Aircraft charterers, sellers, and re-sellers o Art and antique dealers o Auction houses o Other dealers and traders in high value goods o Pawnshops o Travel Agents o Convenience, grocery, liquor stores o Laundromats, car washes, parking businesses o Other cash intensive businesses o Construction companies o Customs agencies and brokers o Mail and courier companies o Hotels o Restaurants and bars o Mining, logging, and other extractive industry companies o Other • Legal persons • Legal arrangements
By inherent characteristics, such as:	• the extent of the sector's economic significance • the complexity of operating structure • the level of integration with other regulated sectors • the sector's scope and accessibility of operations
By products/services, such as:	• information on how sectors, products, services and transactions may be misused for ML • existence of those that facilitate speedy or anonymous transactions

	• cash transactions and cross-border funds transfers • existence of correspondent relationships with banks in high-risk jurisdictions • existence of measures to facilitate tax crimes by non-residents (tax haven)
By customers, such as:	• types and ranges of customers (e.g., percentage of legal persons, percentage of natural persons etc.) • nature of business relationships • existence of higher risk customers, including domestic and foreign PEPs • adherence to regulatory provisions applicable to customers • adherence to any restrictions on customer transaction
By geographies, such as:	• business and customer base in specific geographic areas, including higher risk areas • use of sector by non-residents • customers from geographic area of concerns • adherence to any requirements in other countries • trans-national or cross-border movements of funds and assets • links with business in tax havens
By delivery channels such as:	• the extent to which the delivery of products and services can be conducted with anonymity (including percentage of face-to-face interactions, percentage of non-face-to-face, use of third parties as intermediaries) • complexity (e.g., multiple intermediaries with few immediate controls).

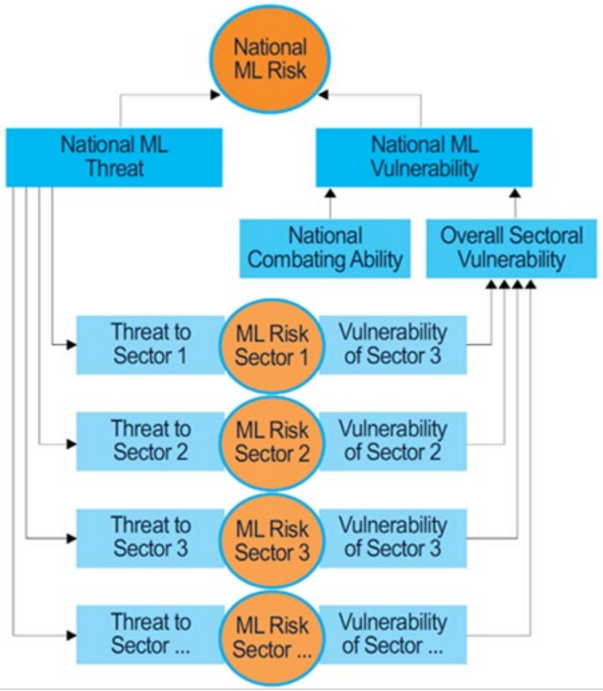
Annex C: Package of NRA Tools

World Bank Tool

The World Bank Tool in Brief

- **Methodology**: A self-assessment tool publicly available online for self-use. One national vulnerability and six sectoral vulnerability modules are based on causal relationship networks inspired by the Bayesian Network. They include built-in assumptions, weights, and pre-conditions. Threat assessment has a top-to-bottom approach that starts with the analysis of threats at the national level and then proceeds to the sectoral level. Vulnerability assessment follows a bottom-up approach from products to sectors, then to the national level. The threat assessment includes the analysis of international threats, in addition to domestic ones. Requires a collection of quantitative and qualitative information and includes supplementary tools for building the capacity for ongoing data collection. The tool deliberately avoids relying on complex statistical calculations since the use of inaccurate, biased, or low-quality data by those without data analysis experience can be misleading. The tool requires qualitative information and expert judgment, in addition to available data. The main role of quantitative data is to support a healthier expert judgment. This approach allows risk assessment even in countries with limited data, due to its flexibility to use qualitative information to fill data gaps. Also, the tool requires consideration of the “unknown” part of the proceeds of crimes, as the statistics on money laundering and predicate offenses represent only the “tip of the iceberg”. Aims to include all relevant national authorities in the process. Requires countries to establish a dedicated NRA working group or task force.

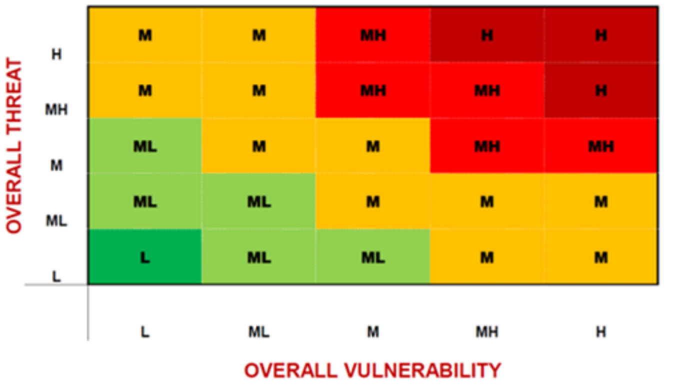
Figure 6. Structure of the World Bank’s Generic ML NRA Tool


National ML Risk
National ML Threat
National ML Vulnerability
National Combating Ability
Overall Sectoral Vulnerability
Threat to Sector 1
ML Risk Sector 1
Vulnerability of Sector 3
Threat to Sector 2
ML Risk Sector 2
Vulnerability of Sector 2
Threat to Sector 3
ML Risk Sector 3
Vulnerability of Sector 3
Threat to Sector ...
ML Risk Sector ...
Vulnerability of Sector ...

Source: Graphic provided by the World Bank

- **Risk is defined as:** A combination of threat and vulnerability at the national and sectoral levels. Threat for ML is a function of proceeds of crime, including those generated by predicate offences and international criminal flows. Analyses predicate offences, typologies, materiality of sectors and other factors.
- **Inherent and Residual risk:** Inherent and residual risk concepts do not exist in the World Bank's Generic NRA Tool. Instead, it has "inherent vulnerability" and "final vulnerability" concepts. The "final vulnerability" is a weighted average of inherent vulnerability and deficiencies in AML controls. Therefore, the AML controls impact the risk level as a part of vulnerability, and the final "risk" levels generated by the tool are "residual risk". As an extension of NRA tool, recently the World Bank has developed a risk monitoring framework for the supervisory authorities. This tool generates both inherent and residual risk level of reporting entities in a sector.
- **Likelihood:** The tool does not include likelihood as a standalone element in risk assessment. However, likelihood is integrated in the design of the vulnerability modules. Likelihood is the basis of Bayesian Networks. The vulnerability modules of the World Bank tool use "cause and effect " and a logical sequence of events like in Bayesian Networks, but they use weights and conditionality instead of probabilities.
- **Consequences:** Included as part of threat and vulnerability assessment rather than as a separate assessment. The methodology assumes that higher threats and vulnerabilities will also lead to higher consequences. In the tool there is an optional template for the assessment of consequences.
- **Risk ratings:** Vulnerability ratings are calculated by the tool based on assessment inputs, as well as the built-in model assumptions, weights, and pre-conditions. Weight and preconditions can be changed by the user countries based on a justification. Threat ratings are determined by expert opinion, which should be supported by qualitative and quantitative information. Pre-defined indicators are provided. In the threat assessment countries can add or change indicators, while this is not possible in vulnerability modules. Threat rating and vulnerability rating are combined in a matrix to give the country's overall risk rating. A second matrix is generated to illustrate the sectoral risks.

Figure 7. World Bank's heatmap to determine overall national risk level

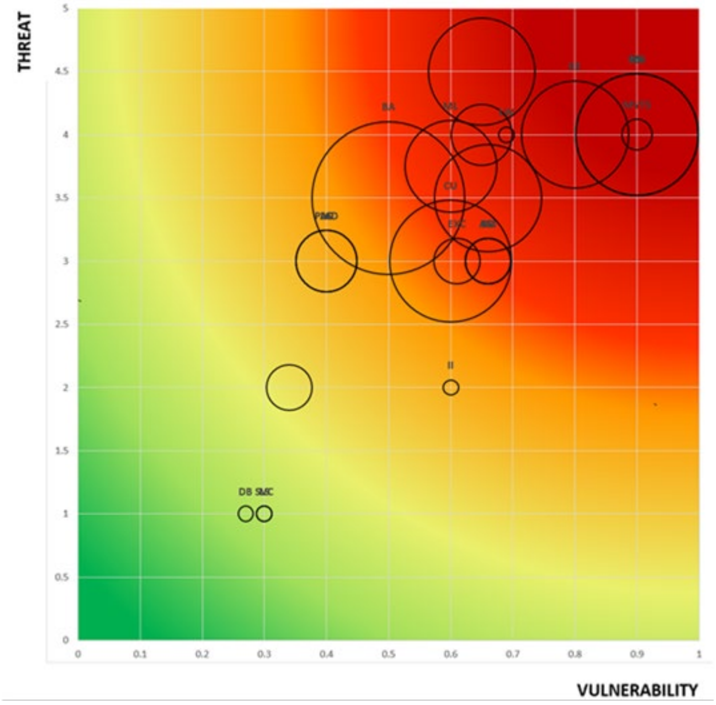


OVERALL THREAT	L	ML	M	MH	H
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M

OVERALL VULNERABILITY

Key: H = high, MH = Medium High, M = Medium, ML = Medium Low, L = Low
Source: Graphic provided by the World Bank

Figure 8. Heat map for ML risks of various sectors (based on scenario entries)



Source: Graphic provided by the World Bank. Please note that this is an example graph, provided for illustrative purposes only – this matrix is generated for countries that use the World Bank's tool to show sectoral risks depending on their specific risk and context.

- **Input required from country:** Self-assessment tools - country coordinates the stakeholders, collects and analyses the information and data, conducts the assessment, fills in the excel templates and documents justifications and evidence for their views. The country is expected to collect the data on ML cases and typologies, proceeds of crime, capacity and effectiveness of government agencies, activities and compliance of reporting entities.

- **Involvement of World Bank:** Provides the tool and excels for completion by country. Provides training, guidance, and review of materials. Risk assessment is done and owned by the country. Countries can have references to the World Bank tool but cannot use the name or logo of the World Bank on their assessment reports or any other documents. Also, these documents should include a disclaimer that explains the limited role of the World Bank team in the assessment. The tool is publicly available, and countries can use the tool without WB technical assistance.
- **Output:** Matrices of overall ML risk in a jurisdiction based on threat and vulnerability, and heatmap of sectoral risks. Country drafts the NRA. The World Bank also provides a risk-based action plan template and guidance on it. The action plan should be completed by the countries.

World Bank Useful Links

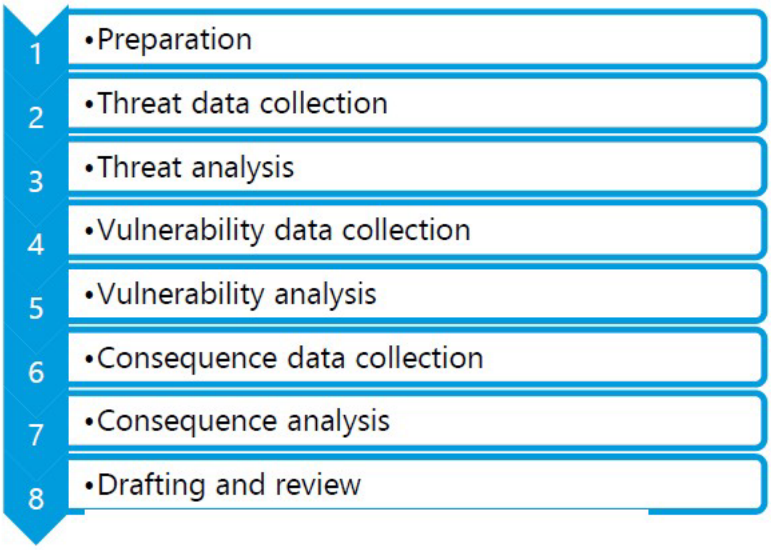
- World Bank Financial Integrity Unit Website *(LINK)*
- Generic National Money Laundering Risk Assessment Tool (2015), Guidance and Training Video *(LINK)*
- Terrorist Financing Risk Assessment Tool (2022), Guidance, and Training Video. (same link as above)
- VA Risk Assessment Tool (2022), Guidance, and Training Video. (same link as above)
- Legal Persons Risk Assessment Tool (2022), Guidance, and Training Video. (same link as above)
- NPO Risk Assessment Tool (2022), Guidance, and Training Video. (same link as above)
- Environmental Crime Proceeds Risk Assessment Tool (2022), Guidance, and Training Video. (same link as above)
- Illicit Financial Flows Data Collection Tool (feeding into ML threat assessment) *(LINK)*., (not public, but available upon request)
- Lessons Learned from the First Generation of Money Laundering and Terrorist Financing Risk Assessments (English). *(LINK)*
- National Assessments of Money Laundering Risks: Learning from Eight Advanced Countries' NRAs *(LINK)*
- A draft framework for money laundering/terrorist financing risk assessment of a remittance corridor (WB-IMF Joint Report), *(LINK)*
- Financial Inclusion Product Risk Assessment Tool and Guidance (2015 - available upon request)
- Risk Assessment Tool for Proceeds of Tax Crimes (2024 –available upon request)
- New version of VA Risk Assessment Tool (available upon request)
- Proliferation Financing (PF) Risk Assessment Tool (available upon request)
- TBML Risk Assessment Tool (currently being developed jointly with UNODC)

International Monetary Fund (IMF) tool

IMF Tool in Brief

- **Methodology:** Designed to be applied in varying degrees of detail depending on country context (i.e., size, complexity, and openness of the financial sector). The risk assessment process is organised around the three key risk components: threat, vulnerability (collectively generating likelihood), and consequence. Data collection is principally conducted through web-based survey tools to collect statistics, and perceptions on the threats, vulnerabilities and consequences in the country. Information is also collected through expert focus groups and validation workshops. All data collection tools and data collected are shared with authorities, so they can continue to the use them to collect data on an ongoing basis. There are eight operational phases of work with some flexibility regarding the number and timing of on-site missions to the jurisdiction:

Figure 9. IMF risk assessment process



1 •Preparation
2 •Threat data collection
3 •Threat analysis
4 •Vulnerability data collection
5 •Vulnerability analysis
6 •Consequence data collection
7 •Consequence analysis
8 •Drafting and review

Source: IMF

- **Risk is defined as:** Likelihood of ML events occurring successfully multiplied by the consequences of those events
- **Inherent and Residual risk:** Methodology measures residual risk ("net risk") - risk remaining after taking into account preventative/mitigating measures and how they reduce risk. (absence of poor controls cannot increase inherent risk, good controls can only reduce it)
- **Likelihood:** Derived from risk analysis modules containing factors, sub-factors, and their indicators. Uses quantitative (data and objective) and qualitative (subjective and perceptions based) indicators from public and private sources. Each module is scored on a 7-point scale, with higher scores equating to higher likelihood that substantial ML abuse will occur successfully

- **Consequences:** Short- and long-term impact of ML abuse successfully occurring. Derived primarily from perceptions of officials, using a structured approach to make informed judgments. Short-term = minimising successful ML over 12-month period, used to analyse sector risk. Long-term = effect of likely level of successful ML on various social/economic/political objectives.
- **Risk ratings:** Semi qualitative focusing on key risk events associated with ML which make a difference to risk profiles. Authorities can add risk events to this.
- **Input required from country:** Requires countries to establish an NRA coordinating mechanism and determine the objectives of the NRA exercise. Surveys on data availability and domestic and transnational ML threat. Fill in Web-based tools providing statistics, and perceptions on the threats, vulnerabilities and consequences in the country. The national authorities are responsible for drafting the NRA.
- **Involvement of IMF:** The IMF provides all data collection tools, the raw analysis, data and a template for the written report. Conduct research into country's proceeds of crime environment and threat indicators. Run capacity-building workshops with authorities. Collect publicly available information on vulnerabilities and threats to generate preliminary risk level rating, collect publicly available information on consequences. Provides a technical assistance report to the country that describes the risk assessment process used and formally conveys the results of the analysis conducted.
- **Output:** Domestic proceeds of crime table. Summary risk matrix. Heat maps for risk events (generic and identified by authorities). Summary tables for sectors and entities. NRA document itself.

Useful links

Please note that IMF tools are not currently public. Links will be shared when available, in the meantime please contact the IMF for further information.

Council of Europe (CoE) Economic Crime and Cooperation Division (ECCD) Tool

CoE ECCD Tool in Brief

- **Methodology**: Adaptable and agile tool designed to guide and support undertaking of initial and review of existing national and sectoral risk assessments. Use and adaptation of process outlined in the tool is based on training and implementation support provided by the CoE ECCD. All CoE ECCD Methodologies,[113] including this tool, are designed to reflect classic risk assessment components, allowing flexibility during the assessment process to take account of data quantity and quality considerations and diversity of sector and subsector risk profiles. Methodology is designed based on a data-

[113] Non-exhaustive list of methodologies developed by the CoE ECCD: ML/TF NRA Methodology, PF NRA Methodology, Sectoral VA and VASP ML/TF risk assessment Methodology, Sectoral TF NPO risk assessment Methodology, Legal persons and legal arrangements ML/TF risk assessment Methodology, ML/TF sectoral methodologies for different sectors of DNFBPs, Organised crime ML/TF risk assessment Methodology, Cross-border ML/TF risk assessment Methodology. All these methodologies comprise data gathering and data analysis tools and are applied on non-for-profit basis, with the support of the CoE ECCD.

driven approach, with sufficient flexibility to incorporate both qualitative and professional judgment-based information, and solution-oriented focus towards the mitigation of calculated residual risks. Approach is designed to identify and challenge assumptions around perceived levels of risk and overall effectiveness of controls intended to mitigate them. Methodology incorporates inclusive and participatory approach through use of national coordinating mechanism, ongoing interaction with both public authorities and the private sector, and robust review of preliminary findings by engaging in structured discussions with the public and private sector (focus groups). Methodology aims to focus assessment findings in a prioritised and risk-based fashion which reflects the country's overall risk appetite, and which is logical, user-friendly and foundational for subsequent national action plans and prioritisation of future work by authorities.

- **Risk is defined as:** A combination of the probability and scope of the consequences - in alignment with *ISO Standard – Risk Management Vocabulary*. In the ML/TF context, risk is defined as the effect of criminal ML/TF capabilities on financial, economic and social objectives.
- **Inherent and Residual risk: Inherent risk** refers to the ML/TF initial risk that exists before any control is applied to address or reduce the impact of that risk. **Residual risk** refers to the level of ML/TF risk that still exists after taking account of both the controls applied to mitigate them and vulnerabilities that may aggravate or maintain the level of risk present. Residual risk refers to the level of risk based upon which country must then determine, based on its risk appetite, the risk treatment it will apply to address those which it determines to exceed its risk appetite.
- **Likelihood:** The judgement on likelihood is proximate to the judgement of the frequency at which criminals may undertake ML taking into account their knowledge and ML skills (based on typologies of cases and precedence) and the strength of preventative and recovery controls. The assessment uses quantitative (data and objective) and qualitative (subjective and perceptions based) indicators from public and private sources.
- **Consequences:** Short- and long-term impact of ML abuse successfully occurring. Derived primarily from perceptions of officials, using a structured approach to make informed judgments. Consequences are assessed based on the effect of likely level of successful ML on various social/economic/political objectives summarised across several impact areas of national and cross-border relevance (e.g. security and rule of law, social, international finance, etc.).
- **Risk ratings:** The CoE NRA and Sectoral Risk Assessment (SRA) methodologies are supported by tools which assist in aggregating initial data to assess inherent risks, support the selection of appropriate scores for likelihood and consequence and evaluate controls and vulnerabilities, to determine final residual risk ratings. The tools are designed to provide both visual and quantitative findings, allowing users to drill down into specific threats and risk areas, as needed. The tool allows users to adjust their own scoring, providing transparency and the ability of customising the rating process, where needed.

- **Input required from country:** Country "owns" the assessment process, leading the establishment of national coordination groups, the identification and collection of data and information and soliciting the active participation of stakeholders from the public and private sector during the assessment process.
- **Involvement of the Council of Europe:** CoE ECCD support is provided through training on how to use the methodology, set up scoring, tool usage, moderation of focus group sessions and to provide "troubleshooting" support throughout the assessment process, as needed. Additional support provided, as requested, for review of draft reports and formulation of preliminary action plans, to reflect both country's risk appetite and overall risk-based approach towards mitigation of ML/TF risks.
- **Output**: ML/TF NRA Report with interactive matrix and heat map showing preliminary and final assessment results; summary tables to support concise recording of findings ("risk events") from each risk area assessed. Risk mitigation and monitoring tool (basis for the Action Plan) template is integral part of the Methodology.

Useful Links

- Home page: - Risk Assessment Tools - Welcome to the Economic Crime and Cooperation Division - Economic Crime and Cooperation Division
- Contact Information: contact.econcrime@coe.int

Other sources for consideration

NRAs and sectoral/thematic risk assessments that have been sent to the FATF Secretariat by delegations can be found on the RTMG Community workspace: Library of ML/TF/PF Risk Assessments (this link is not public).

Countries should assess the reliability of all sources consulted and be aware of potential biases. As stated throughout this guidance, sources listed are non-exhaustive and should not replace data collection and analysis on a national level. Rather, the goal is to provide a variety of sources for background information that can support jurisdictions in the initial stages of research on their risks. This list is non-exhaustive.

Table 10. Corruption sources

Source	Link
APG	• PILON/APG Typologies Report - Recovering the Proceeds of Corruption in the Pacific (2016)
ESAAMLG	• Procurement Corruption in the Public Sector and Associated Money Laundering in the ESAAMLG Region (2019)
FATF	• FATF report on Laundering the Proceeds of Corruption (2011) • Specific Risk Factors in the Laundering of Proceeds of Corruption (2012) • FATF Guidance on Politically Exposed Persons (2013)
GIABA	• Money Laundering and Terrorist Financing through Corruption in West Africa (2022)
MENAFATF	• Money Laundering and Corruption (2017)
UN	• UNCAC - United Nations Convention against Corruption • Thematic Areas in Anti-Corruption • Implementation Review Mechanism • Country Profiles • Legal Library
UNODC	• UNODC SHERLOC database
World Bank	• "Control of Corruption" statistics and other governance indicators such as on "Rule of Law", "Governance Effectiveness", and "Regulatory Quality" (Home | Worldwide Governance Indicators) • Transparency, accountability and corruption in the public sector • IDA Resource Allocation Index • Enterprise Surveys – Corruption Perceptions
Other	• Organised Crime and Corruption Reporting Project • IDEA Global State of Democracy Indices • State Capture Matters: A research article and associated dataset and index | Results for Development

Table 11. VA/VASP sources

Source	Link
CFATF	• ML/TF risks through the use of VA/VASP (2023)
EAG	• Legalization (laundering) of the proceeds of cybercrime, as well as financing of terrorism from the said offence, including through the use of electronic money or virtual assets and the infrastructure of their providers (2022)
Egmont Group of FIUs	• Emerging Financial Technologies ML and TF: A Typology of Virtual Currencies (2018)
ESAAMLG	• The Opportunities and Challenges Posed by VA/VASPs in the ESAAMLG region (2024)
FATF	• FATF's 2024 Targeted Update on the Implementation of the FATF Standards on VA and VASPs (2024)

	• Updated Guidance for a Risk-Based Approach for VA and VASP (2021) • Virtual Assets red flag indicators of ML and TF (2020)
MONEYVAL	• ML and TF Risks in the world of VA (2023)
OECD	• International Standards for International Exchange of Information
UNODC	• UNODC SHERLOC database
Open-source[114]	• Coindesk - reports on VA trends. • BestChange- open-source site on P2P exchange options • CoinTelegraph - reports on VA trends • CoinMarketCap - Open-source info on top VA exchangers by trading volume • Coin ATM Radar - map of VA ATMs
Private sector[115]	• TRM Labs • Lukka • Chainalysis • Elliptic • Merkle Sciences

Table 12. Legal Persons and Legal Arrangements Sources

Source	Link
CFATF	• Vulnerabilities in the concealment of beneficial ownership information (2021)
FATF	• Guidance on BO Transparency of Legal Persons (2023) • Guidance on BO Transparency of Legal Arrangements (2024) • TBML: risk indicators (2021) • FATF Laundering the Proceeds of Corruption (2011)
GIABA	• Beneficial Ownership Information and Asset Recovery Framework in West Africa
IMF	• Unmasking Control: A Guide to Beneficial Ownership Transparency (2022)
OECD	• OECD Agreement on Exchange of Information in tax matters • OECD Automatic Exchange Portal
UNODC	• UNODC SHERLOC database
World Bank	• The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It (2011) • Signatures for Sale: How Nominee Services for Shell Companies are Abused to Conceal Beneficial Owners (2022)
Other	• Tax Index

[114] Countries should not take such reports at face value, and to evaluate the reliability of the source. These are shared to build background information and understanding.

[115] Ibid.

Table 13. Informal Economy Sources

Source	Link
FATF	- The role of Hawala and other similar service providers in ML/TF (2013) - Guidance on Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures (2025)
GAFILAT	- Analysis of Regional Threats on ML (2015)
IMF	- Shadow Economies Around the World: Size, Causes, and Consequences - WP/00/26 (2000)
OECD	- Informality and globalisation (2023) - Vulnerability in the informal economy (2019) - Measuring the non-observed economy: a handbook (2002)
World Bank	- Informal Economy Database - Global Findex Database
UN	- Informal Economy database - Recommendation R204 - Transition from the Informal to the Formal Economy Recommendation, 2015 (No. 204)

www.fatf-gafi.org

August 2025