

A hand holding a smartphone displaying a financial candlestick chart with a moving average line. The background is a blurred image of a hand holding a smartphone with a similar chart.

NATIONAL MONEY LAUNDERING / TERRORIST FINANCING RISK ASSESSMENT TOOLKIT

GUIDANCE MANUAL

AML/CFT NATIONAL RISK ASSESSMENT ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS



Funded by the European Union



WORLD BANK GROUP

© 2025 International Bank for Reconstruction and Development / The World Bank
1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent.

The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, links/footnotes and other information shown in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The citation of works authored by others does not mean the World Bank endorses the views expressed by those authors or the content of their works.

Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

Rights and Permissions

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

Any queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e-mail: pubrights@worldbank.org.

Cover photo: © Adam Śmigielski / Unsplash



Contents

Disclaimer and Terms of Use	5
Acknowledgments	6
Abbreviations and Acronyms	7
1. Introduction	8
1.1. Context: Virtual Assets and Money Laundering (ML) and Terrorist Financing (TF) Risks	8
1.2. The Risk Assessment Tool	9
1.3. Purpose and Structure of This Guidance	10
1.4. Key Definitions	10
2. Risk Assessment Process	12
2.1. Working Group and Focal Point	12
2.2. Training	14
2.3. Substantive Scope of Risk Assessment	14
2.4. Initial Data Collection	16
2.5. Selecting the Appropriate Module Tier	17
2.6. Entering Inputs	18
2.7. Analyzing Output	19
2.8. Next Steps	19
3. Guidance on Completing Tool Inputs	20
3.1. Step 1: Scoping and Mapping	21
3.2. Step 2: ML and TF Threat Assessment	30
3.3. Step 3: National Vulnerabilities	37



Contents

3.4. Step 4: National Mitigation Measures	43
3.5. Step 5: Specific VA and VASP Assessments	46
4. Tool Outputs	63
4.1. Output 1: Risk Overview	63
4.2. Output 2: ML Cases	65
4.3. Output 3: Techniques	66
4.4. Output 4: Criminal Use of VAs	67
4.5. Output 5: Technical Compliance	68
4.6. Output 6: Preventive Measures for VASPs	69
4.7. Outputs 7a to 7f: Specific VA and VASP Types	70
4.8. Outputs 8a and 8b: DeFi and CeFi	71
5. Glossary	73
6. Related FATF Documents	77
ANNEX 1. Decision Tree for Tier Selection Quiz	78
ANNEX 2. Examples Illustrating ML/TF Techniques	79
Notes	84



Disclaimer and Terms of Use

The National Money Laundering/Terrorist Financing Risk Assessment (NRA) Toolkit has been developed by World Bank Group (WBG) staff members to support WBG client countries and jurisdictions in self-assessing their money laundering and terrorist financing risks. The NRA Toolkit contains guidance manuals, including this document; Excel worksheets and the formulas therein; PowerPoint presentations; and any other materials provided as part of the NRA Toolkit. Jurisdictions are advised to use the NRA Toolkit with technical assistance from the WBG to ensure proper application.

The NRA Toolkit is supplied in good faith and is based on certain factors, assumptions, and expert opinions that the WBG may in its absolute discretion have considered appropriate at the time the toolkit was developed. Even if being done through the NRA Toolkit, an NRA is conducted as a self-assessment by a jurisdiction and not by the WBG staff. The user is responsible for any data, statistics, and other information put into the various NRA Toolkit templates, as well as for any interpretation and conclusion based on the results of the NRA Toolkit.

The WBG provides the NRA Toolkit as is and disclaims all warranties, oral or written, express or implied. That disclaimer includes without limitation a warranty of the fitness for a particular purpose or noninfringement or accuracy, completeness, quality, timeliness, reliability, performance, or continued availability of the NRA Toolkit as a self-assessment tool. The WBG does not represent that the results derived from the NRA Toolkit are complete or applicable to a user's circumstances and accepts no liability in relation thereto. The WBG shall not have any liability for errors, omissions, or interruptions of the NRA Toolkit.

The WBG will not be responsible or liable to users of the NRA Toolkit or to any other party for any information or results derived from using the NRA Toolkit for any business or policy decisions made in connection with such usage. Without limiting the foregoing, in no event shall the WBG be liable for any lost profits—direct, indirect, special, incidental, or consequential—or any exemplary damages arising in connection with use of the NRA Toolkit, even if notified of the possibility thereof. By using the NRA Toolkit, the user acknowledges and agrees that such usage is at the user's sole risk and responsibility.

The NRA Toolkit does not constitute legal or other professional advice, but in particular it does not constitute an interpretation of these Financial Action Task Force (FATF) documents: *FATF 40 Recommendations and Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems*. The WBG shall not be responsible for any adverse findings, ratings, or criticisms from the FATF or FATF-style regional bodies arising from use of the NRA Toolkit.

Nothing herein shall constitute or be considered a limitation on or a waiver of the privileges and immunities of the International Bank for Reconstruction and Development, which are specifically reserved.



Acknowledgments

This tool has been developed by the Financial Market Stability and Integrity (FSI) unit of the World Bank. The tool and this guidance were developed by Ailsa Hart (project team lead), Olivier Kraft (World Bank AML/CFT consultant), and Mark McGoldrick (World Bank AML/CFT consultant). The team is especially grateful to the peer reviewers for their time and expertise: Matei Dohotaru (Senior Financial Sector Specialist, World Bank), Danny Sougith Sanhye (Senior Forensic Accountant, World Bank), Joseph Oliver Eloi (World Bank AML/CFT consultant), Janet Ho (UK's Financial Conduct Authority), David Baker (Isle of Man Financial Services Authority), Caroline Horres (US Treasury), and the Financial Action Task Force Secretariat, TRM Labs, and Blocktrace. Comments were provided in a personal capacity and do not necessarily represent the views of the respective organizations. Their thoughtful comments and constructive feedback were critical in the development of this tool and significantly improved early versions.



Abbreviations

AML	anti-money laundering
CDD	customer due diligence
CeFi	centralized finance
CFT	countering the financing of terrorism
DeFi	decentralized finance
DNFBP	designated nonfinancial business and profession
FATF	Financial Action Task Force
FIU	financial intelligence unit
FSB	Financial Stability Board
ICO	initial coin offering
IOSCO	International Organization of Securities Commissions
KYC	know your customer
ML	money laundering
NRA	national risk assessment
OECD	Organisation for Economic Co-operation and Development
OTC	over the counter
P2P	peer-to-peer
PEP	politically exposed person
PF	proliferation financing
STR	suspicious transaction report
TF	terrorist financing
VA	virtual asset
VASP	virtual asset service provider



1. Introduction

1.1. Context: Virtual Assets and Money Laundering (ML) and Terrorist Financing (TF) Risks

Virtual assets (VAs)¹ represent a growing source of innovation in the global financial system, offering new possibilities for value transfer and digital inclusion. This rapid evolution is shown by the global VA market reaching a record valuation of \$4 trillion in July 2025.² Alongside this growth, VAs also present unique characteristics such as pseudonymity, speed of cross-border transactions, and technological complexity that challenge traditional regulatory and supervisory approaches.

The Financial Action Task Force (FATF)—the global standard setter for anti-money laundering (AML) and countering the financing of terrorism (CFT)—has emphasized the need for jurisdictions to assess and understand the financial crime risks for this sector. A comprehensive assessment of the money laundering/terrorist financing (ML/TF) risks related to VAs and virtual asset service providers (VASPs)³ enables a proportionate, risk-based response to regulation, ensuring that resources are deployed where they are most needed and that legitimate innovation is not unnecessarily hindered. In 2019, FATF extended its AML/CFT standards to cover VAs and VASPs through amendments to Recommendation 15 on new technologies. The revised FATF Recommendation 15 requires jurisdictions to ensure that VASPs are subject to AML/CFT obligations, including licensing or registration, customer due diligence (CDD), and transaction monitoring.⁴ The United Nations, the Financial Stability Board (FSB), the Organisation for Economic Co-operation and Development (OECD), and other international bodies have similarly recognized the pressing need for proportionate financial regulation of virtual assets.⁵

1.2. The Risk Assessment Tool

The World Bank has developed an updated VA and VASP risk assessment tool to support national authorities in systematically identifying and assessing the ML/TF risks associated with VAs and VASPs. The tool responds to the rapidly evolving standards and technologies in this space.

Since 2022, the World Bank has supported over 20 jurisdictions with both low and high capacities in conducting such assessments, and insights from this experience have informed the revision of this tool.

This revised tool has three tiers: basic, intermediate, and advanced. The tiered approach reflects the World Bank's experience working with jurisdictions at varying stages of capacity and market development. It allows jurisdictions to use a version that aligns with their needs, resources, and the maturity of their VA/VASP sector. The revised version also reflects the fact that jurisdictions now have access to more data on VASP activities and business practices than in 2022 and can therefore answer more quantitative questions. It also integrates new ML/TF techniques and typologies which have emerged in recent years. Jurisdictions interested in assessing proliferation financing (PF) risks involving VAs should refer to the World Bank's separate methodology for PF risk assessments.

The risk assessment tool is an Excel-based workbook that guides jurisdictions through a multistep process, summarized in figure 1.

>>>

Figure 1.1 Overview of Steps of the Risk Assessment Tool



Note: ML = money laundering; TF = terrorist financing; VAs = virtual assets; VASP = virtual asset service providers.

1.3. Purpose and Structure of This Guidance

This document provides instructions for conducting a risk assessment using the World Bank’s updated VA and VASP risk assessment tool. By following the step-by-step approach outlined in this document, jurisdictions can gain the most value from the tool and obtain actionable insights to inform their regulatory and enforcement responses to ML/TF risks in the VA/VASP sector.

The guidance consists of the following chapters:

- **Risk Assessment Process:** This chapter explains the overall process for conducting a risk assessment using the tool, from forming the working group to completing the data collection and interpretation.
- **Tool Inputs:** This chapter provides detailed instructions for completing the input tabs of the tool, including both qualitative and quantitative questions.
- **Tool Outputs:** This chapter explains how to interpret the output tabs of the tool, including visualizations, risk summaries, and tables, to support decision-making and inform AML/CFT strategies.
- **Glossary:** This chapter defines key terms and concepts used in the guidance and tool.

Note: While the tool provides a structured framework for analysis, it is not a substitute for expert judgment. Outputs must be interpreted within the specific context of each jurisdiction’s legal, regulatory, and operational environment. In addition, limitations in data availability can affect the risk assessment. Intelligence and data limitations should therefore be documented and considered when drawing conclusions.

1.4. Key Definitions

While there is a full glossary at the end of the document, table 1.1 defines a small set of terms for ease of reference. Authorities are also encouraged to maintain their own list of definitions relevant to international standards, national laws, guidance, and implementing regulations.

>>>

Table 1.1 Key Definitions

Input	Guidance
Virtual asset	<p>This World Bank risk assessment tool uses the following FATF definition of a virtual asset: “a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. VAs do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations” (FATF Glossary, https://www.fatf-gafi.org/en/pages/fatf-glossary.html; emphasis added).</p> <p>See additional guidance on defining the scope of virtual assets in section 2.3. Notably, the definition here includes virtual assets that may be considered as both securities or wider tokenized financial instruments when used for payment or investment purposes.</p>

Virtual asset service provider (VASP)	<p>This World Bank risk assessment tool uses the FATF's definition, which considers VASPs to be "any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:</p> <ul style="list-style-type: none"> i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets [on behalf of another natural or legal person]; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset" (FATF Glossary). <p>Given the fast-evolving nature of the VA sector and differences in national definitions, the World Bank's risk assessment tool provides flexibility for jurisdictions to scope in additional VA services and products as appropriate.</p>
Domestic VASP	Any VASP that is licensed or registered under the jurisdiction's law or regulations, and/or any company or individual based in the jurisdiction which is offering VA services on behalf of another natural or legal person. This can include VASPs headquartered in another jurisdiction that have obtained a local license or registration.
Foreign VASP with material local presence	A VASP with a material local presence that is not licensed or registered in the jurisdiction, and not legally established in the jurisdiction. A material local presence can be determined on the basis of a market survey indicating that a VASP has a material customer base in the jurisdiction or that a VASP's marketing materials target consumers in the jurisdiction. A foreign VASP may be regulated by a third jurisdiction or not regulated at all.
ML/TF threat	<p>In the context of VAs, an ML/TF threat refers to individuals or entities seeking to exploit VAs or related services to conceal the illicit origin of funds or in support of terrorism. Examples:</p> <ul style="list-style-type: none"> • Cybercriminal extorting VAs from victims • Organized crime group generating cash proceeds and converting them into VAs • Individuals converting funds into VAs to support terrorist fighters in another jurisdiction
ML/TF vulnerability	<p>Vulnerabilities refer to factors that make a jurisdiction, a sector, or a particular service attractive for ML or TF, and that can be exploited by threat actors. Certain vulnerabilities may be inherent to a sector or product, whereas other vulnerabilities may be caused by national gaps or weaknesses. Examples:</p> <ul style="list-style-type: none"> • Weaknesses in national law enforcement capacity to trace and follow criminal proceeds in virtual assets • Provision of high-risk products by local VASPs
ML/TF risk	<ul style="list-style-type: none"> • ML/TF risk refers to the potential for ML and TF threats to exploit vulnerabilities within a jurisdiction or an organization's financial system.

Note: FATF = Financial Action Task Force.



2. Risk Assessment Process

This chapter explains the overall process that a jurisdiction should take when conducting a risk assessment, from forming the working group to completing the data collection and interpreting the results.

2.1. Working Group and Focal Point

When conducting a virtual asset risk assessment, jurisdictions should nominate a designated focal point and lead agency to coordinate the process and should establish a multiagency working group. This multiagency structure is vital to ensuring coordination and accountability and enables the integration of diverse perspectives.

The VA/VASP risk assessment may be conducted either as part of a wider national risk assessment or as a standalone assessment. Each option has pros and cons. An integrated approach means that the jurisdiction can take a more holistic approach to understanding risk and thus can draw on the latest information on national ML/TF threats and vulnerabilities when forming its assessment of the VA sector. However, a standalone assessment may be appropriate if the jurisdiction wants to go into more depth or needs to follow a specific timeline for the virtual asset assessment. A dedicated working group on VAs should be formed in either scenario.

Focal Point

A designated lead agency and focal point should manage and coordinate the assessment process. This role can be held, for example, by an official within the national AML/CFT coordination body, the financial intelligence unit (FIU), or the lead supervisory authority. The focal point is responsible for the following tasks:

- Coordinating the establishment and activities of the working group
- Overseeing the assessment process and ensuring adherence to timelines
- Managing quality control and ensuring proper documentation of findings
- Serving as the primary liaison with external stakeholders

Composition of the Working Group

The VA/VASP Risk Assessment Working Group should draw on the expertise of key institutions involved in AML/CFT efforts at the national level (and at the regional or subnational level if applicable). The size of the working group will differ depending on the jurisdiction's context, but it generally should not exceed more than 50 representatives, to keep the coordination manageable. While the composition of the working group will depend on the jurisdiction's specific context, experience to date shows benefits of including both public and private sector perspectives. See the following suggestions on the composition of the working group.

Public sector core agencies:

- Supervisory bodies for VAs and VASPs, if appointed
- The FIU
- Law enforcement and intelligence agencies—ideally, investigators with experience in working on ML, TF, sanctions evasion, or predicate cases that involve virtual assets
- Public Prosecutor's Office or Attorney General's Office
- Other financial supervisors and supervisors of designated nonfinancial business and professions (DNFBPs) listed in the FATF Standards.
- Representatives from the central bank, if not already covered
- Tax and revenue authority, including any authorities with experience working on combatting tax evasion or tax crimes involving virtual assets
- Ministry of Justice or other agencies responsible for handling international cooperation requests (mutual legal assistance, extradition, and so on)
- Anticorruption authority, if any

Public sector additional agencies:

- Customs authority
- Subnational authorities, as applicable, such as provincial prosecutors or local regulators in federal systems

The final decision on ratings should be taken collectively by the working group, although specific subtasks may be assigned to individual members. For example, the FIU and law enforcement authorities typically focus more on the assessment of ML/TF threats, while the supervisors may focus more on the assessment of ML/TF vulnerabilities.

Engagement with Private Sector, Civil Society, and Academia

The involvement of representatives from the private sector, civil society, and academia can provide valuable perspectives on the VA/VASP sector, market trends, and emerging risks. The decision on whether to include such representatives in the formal working group or through separate consultations will depend on the specific jurisdiction's context and the depth of local private sector expertise. At a minimum, jurisdictions should ensure that they seek private sector inputs at critical stages in the assessment to validate findings (such as at the initial data collection stage, when developing preliminary findings, and when drawing final conclusions, including recommendations for follow-up actions to address identified risks).

Relevant stakeholders may include the following:

- VA industry representatives or associations (such as exchangers, wallet providers, stablecoin issuers, and other types of VASPs)
- Blockchain analytics companies that can supply data on jurisdiction-specific trends
- Representatives or associations of representatives of the traditional financial sector (given the direct or indirect exposure to VAs)
- Academics with expertise in financial crime prevention, virtual assets, or emerging technologies
- Civil society organizations with a focus on AML, financial integrity, or related issues

- Independent experts in AML/CFT, anticorruption, or economic crime
- Consumer protection or fraud victim support groups

Engagement with nongovernment stakeholders should ensure the confidentiality of sensitive data, particularly information related to law enforcement and intelligence. Jurisdictions interested in receiving more detailed good practices and assistance to review data collection questionnaires should reach out to the World Bank team.

2.2. Training

A successful VA/VASP risk assessment depends on the relevant expertise and capacity of all working group members. All members should have a sufficient understanding of VAs; VASP businesses, products, and practices; the associated ML and TF risks; or a combination of these. It may be preferable to include analyst- or investigator-level staff in the working group rather than management-level members, depending on who is most familiar with these topics.

Jurisdictions are encouraged to invest in targeted training for working group members as needed. This may include the following:

- Introductory sessions on the VA ecosystem, including VASP businesses, products, and practices, and key technologies
- Briefings on regulatory and supervisory frameworks for VASPs
- Best practices for supervision and enforcement
- Case studies and typology reviews illustrating ML/TF risks in the VA sector

Jurisdictions should consider whether training can be delivered best by domestic authorities that have had more exposure to VAs, by external providers, or both. The working group membership should be reassessed following the training because members may identify other authorities whose input may be required.

In addition, the World Bank offers training on virtual assets and the use of the risk assessment tool itself. This training covers all areas discussed in this guidance:

- Risk assessment process
- How to navigate the tool
- Best practices for entering data and interpreting outputs

For wider World Bank resources on risk assessments, please refer to the World Bank's public NRA site: <https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use>.

2.3. Substantive Scope of Risk Assessment

After forming the working group, members should discuss the intended objectives and scope of the assessment (that is, the time period that the assessment will cover and the scope of VA and VASP activities that will be considered). The global AML/CFT requirements oblige jurisdictions to understand their ML and TF risks related to both virtual asset service providers and virtual asset coins, services, and products more broadly.

Scope of Virtual Assets

Typically, when deciding on the scope of virtual assets to include for an ML/TF risk assessment, jurisdictions would want to include the following:

- Cryptocurrencies (such as Bitcoin,⁶ Ether,⁷ and Monero⁸)
- Stablecoins, which are virtual assets whose value is pegged 1:1 with another asset, typically a fiat currency (such as Tether,⁹ USD Coin,¹⁰ and DAI¹¹)
- Certain utility and governance tokens when used for investment or payment purposes (such as Basic Attention Token¹² and Chainlink,¹³ subject to how they are used in practice and the applicable regulatory framework)
- Non-fungible tokens (NFTs),¹⁴ when used for payment or investment purposes. (Given that many NFTs have hybrid characteristics, jurisdictions may wish to take an inclusive approach when covering NFTs for assessment purposes.)
- Other types of virtual assets when used for investment or payment purposes, such as wrapped/bridged assets (which are assets that represent another asset on a different blockchain)

The following are generally excluded from the scope of ML/TF risk assessments (although jurisdictions may still choose to include such assets):

- Central bank digital currencies (CBDCs)¹⁵
- Securities regulated under other legal frameworks
- Loyalty points and in-game assets that cannot be converted into fiat currency¹⁶
- Tokenized deposits¹⁷

The working group should adapt the scope of its assessment depending on the local market context and should clearly document and justify the reason for including or excluding any specific VA types, services, or activities. In line with FATF guidance, jurisdictions should adopt a functional approach when deciding whether a certain token is within scope (thus this decision should be based on the function served by the token in practice rather than on the terminology or marketing terms used).

Scope of Virtual Asset Service Providers

The same scoping exercise should be conducted with respect to the VASPs. The World Bank recommends that, at a minimum, jurisdictions assess the ML/TF risks associated with all activities identified under the FATF VASP definition, which includes the (a) exchange or transfer of virtual assets, (b) safekeeping or administration of virtual assets, or (c) participation in and provision of financial services related to an issuer's offer or sale of a virtual asset, or both.

In addition, the World Bank's tool encourages jurisdictions to consider the ML/TF risks related to broader virtual asset services and actors. This category includes ML/TF risks linked to mixing and tumbling services, which commingle and pool together VA transactions, therefore obscuring the trail back to the original source of funds. Similarly, the World Bank risk assessment tool encourages jurisdictions to consider the interaction between VAs, VASPs, and traditional financial institutions. This effort would include an assessment of the extent to which banks may be servicing VASP clients or clients who are trading in VAs.

Prohibitions on VAs or VASPs

Even when jurisdictions choose to prohibit VAs or VASPs, the FATF's Recommendation 15 still requires the jurisdictions to conduct a thorough assessment of their ML and TF risks related to this sector. This assessment includes the ML/TF risks from misuse of unlicensed or unregulated providers in the jurisdiction, or misuse of foreign VASP companies to launder criminal funds generated within the jurisdiction. Given this requirement to still conduct a thorough risk assessment, jurisdictions that prohibit VAs and VASPs should still complete all steps of the World Bank's VA risk assessment tool.¹⁸

2.4. Initial Data Collection

To help inform the working group's decision on the scope of the assessment, the members should gather information on relevant local VA laws and regulations, as well as information from the working group members on the materiality of virtual assets and VASP activity. This initial data collection will also help the working group determine the appropriate module (basic, intermediate, or advanced) and inform subsequent analysis.

For the subsequent stages of the assessment (the mapping, ML/TF threat, vulnerability, and mitigation assessments), the working group will need to conduct a more thorough data collection exercise. A list of relevant primary and secondary information sources for jurisdictions is provided in the rest of this section. For more detailed guidance on what information should be collected for each stage of the assessment, refer to chapter 3 of this guide.

Official Primary Data Sources

Official primary data sources include the following:

- Legal and regulatory provisions related to VAs and VASPs
- Any previous national or regional risk assessments on virtual assets and VASPs
- The latest NRA on money laundering and terrorist financing
- Supervisory and registration data on VASPs (such as the number, types, and activities of providers; compliance records; sanctions; unlicensed VASPs; and unregulated activities)
- FIU data, including suspicious transaction reports (STRs) related to VAs or VASPs
- Law enforcement and intelligence data (such as investigations, prosecutions, and asset seizures involving virtual assets)
- Tax and customs data (such as cross-border flows, undeclared assets, and investigations involving virtual assets)
- Data held by the central bank (for example, on national virtual asset adoption)
- Data on international cooperation involving virtual assets (including any informal requests, or mutual legal assistance/extradition requests with references to VAs)
- Information provided by VASP industry representatives or associations on their clients, products, and services, or data from the financial sector, such as bank and payment operators on VA activities

Additional Secondary Sources of Information

Data held by working group institutions should be complemented by additional secondary sources, which may provide valuable insights on market trends, typologies, and emerging risks. These may include the following:

- Reports from the FATF and FATF-Style Regional Bodies, such as
 - The latest assessment of the jurisdiction's technical compliance with FATF's Recommendation 15
 - The jurisdiction's most recent mutual evaluation report and follow-up reports
 - Typology reports
- Findings from the World Bank/International Monetary Fund Country Financial Sector Assessment Program if the assessment covered AML/CFT, virtual assets, or both
- Public or regulatory reports from foreign authorities on supervision or compliance of foreign VASPs (and particularly those that are operating within the jurisdiction conducting the risk assessment)
- Publications by blockchain analytics firms
- Academic research on the VA sector and financial crime
- Market reports from industry or trade associations
- Investigative journalism and reliable media reports

The working group should assess the reliability and relevance of all data sources, document any data gaps or limitations, and

consider these factors when interpreting results. When assessing reliability and accuracy, the working group should bear in mind that *data sources related to VAs can become outdated quickly*.

Time Period for Data Collection

The working group should agree on the period to be covered by the assessment. A time frame of the past four years is generally recommended because it allows for the identification of trends over time.

2.5. Selecting the Appropriate Module Tier

The tool includes a short quiz to assist the working group in selecting the most suitable version of the risk assessment tool: basic, intermediate, or advanced. The quiz is designed to provide a high-level recommendation of the most appropriate tool based on the jurisdiction’s context, including the size and complexity of the VA sector, the regulatory framework in place, and experience with VA risk assessments.

The basic version is aimed at jurisdictions with limited VA activities, whereas the intermediate and advanced versions are aimed at jurisdictions with progressively more advanced VA ecosystems. While the basic tier enables jurisdictions to assess core VA and VASP services (with a focus on exchangers and wallet services), the intermediate and advanced tiers include a more in-depth assessment of additional ML/TF techniques and VA services, including ML/TF risks linked to decentralized finance (DeFi).¹⁹ See an overview of the key differences in figure 2.1.



Figure 2.1 Overview of the Differences across the Basic, Intermediate, and Advanced Modules



Although the quiz generates a recommendation based on the answers provided, the final decision on which version to use should be based on the collective judgment of the working group, taking into account the specific context and capacity of the jurisdiction.

Further details on the quiz are provided in chapter 3 of this guide.

2.6. Entering Inputs

Once the module has been selected, the working group should complete the relevant input tabs. The input tabs are organized into five steps which feed into each other (as shown in table 2.1). Certain tabs have different levels of detail depending on the module level, with the advanced tier including additional assessment steps.

A detailed explanation of how to complete these inputs is provided in chapter 3 of this guide.

When completing the assessment and tabs, it is important that the working group maintains a quality control process. This requirement could include a process to review or validate inputs before analysis (such as through a peer review or review from foreign counterparts).

>>>

Table 2.1 Overview of Key Steps in the World Bank's VA and VASP Risk Assessment

Step	Tabs
Step 1: Scoping and Mapping	Module Selection Quiz
	Home
	Definitions
	General Mapping
	Optional: Entity Mapping [advanced module only]
	Optional: VA Mapping [advanced module only]
	Case Studies
Step 2: Threat Assessment	National ML and TF Threats
	ML and TF Techniques
Step 3: Vulnerability Assessment	National Inherent Vulnerability
Step 4: Assessment of Mitigation Measures	National Mitigation Measures

Step 5: Specific VA and VASP Assessments	VA Types
	Exchangers
	VA Wallets
	VA Investments [advanced and intermediate modules only]
	Other Services [advanced and intermediate modules only]
	Regulated Entities (non-VASP)

2.7. Analyzing Outputs

The risk assessment tool includes output tabs that generate visualizations and summaries based on the information entered in the input tabs. These outputs provide an initial overview of the ML/TF risks associated with virtual assets and VASPs in the jurisdiction.

A detailed explanation of how to read and interpret these outputs is provided in chapter 4 of this guide.

Although the outputs provide a useful starting point for analysis, they should be considered as indicative results, rather than final conclusions. The working group is encouraged to use the outputs as a basis for consultations with relevant stakeholders (such as workshops with key agencies or industry representatives). Engaging stakeholders in reviewing the outputs helps ensure a more robust and comprehensive understanding of the risk landscape.

Following these consultations, the working group should prepare a report that presents the findings of the risk assessment. The report should combine the outputs from the tool with additional insights gathered through stakeholder discussions, expert input, and contextual analysis. It should clearly document key risk areas, sectoral vulnerabilities, and any data gaps.

2.8. Next Steps

Once a jurisdiction has determined the level and nature of ML/TF risks, it is vital that the jurisdiction then develop an action plan which outlines concrete steps to address and mitigate the risks identified. This plan may include legislative reforms, enhancements to regulatory and supervisory frameworks, targeted outreach to high-risk sectors, capacity building for relevant agencies, or further data collection and analysis. The action plan should include a clear timeline for implementing these measures as well as a monitoring mechanism.

Authorities should also consider how to disseminate the findings of the assessment to relevant stakeholders. This effort may include engaging the private sector through targeted consultations and sharing a summary of key findings with a wider audience.

The risk assessment is not a one-time exercise. Authorities are encouraged to establish a process for periodic and ongoing discussions of risk, particularly as the VA sector evolves, new technologies emerge, or additional data become available. The risk assessment process should be repeated at least every four years, building on the previous assessment. Regular updates will help ensure the assessment remains relevant and continues to inform effective national AML/CFT strategies and supervisory practices.



3. Guidance on Completing Tool Inputs

This chapter provides detailed instructions on how to complete the assessment steps. It can also be used as a working document to inform the division of responsibilities among working group members and to keep track of progress.

3.1. Step 1: Scoping and Mapping

The first step in the World Bank's risk assessment tool is the mapping and scoping exercise. This is composed of three key substeps:

- **Step 1.1. Completing a short quiz to inform the working group's decision on which version of the tool** (basic, intermediate or advanced) is most appropriate for the jurisdiction's context.
- **Step 1.2. Qualitative scoping and mapping on the materiality of virtual assets and VASPs in the jurisdiction**, including any relevant definitions.
- **Step 1.3. Quantitative scoping and mapping, including gathering statistics and case studies on ML/TF risks related to VAs and VASPs.**

Detailed guidance on each of these substeps is included in this section, along with two additional optional steps for jurisdictions that are completing the advanced version of the tool. The optional steps are a more detailed mapping exercise of the types of (a) VAs being traded in the jurisdiction and (b) the specific VA companies operating in the jurisdiction. For jurisdictions conducting the advanced version, see guidance on substep 1.4.

Step 1.1. Module Selection Quiz

Using the "Module Selection" tab of the Excel tool, jurisdictions should answer the quiz to inform the working group's decision on which tier is most suited to the jurisdiction's risk profile and capacity. The working group should begin by answering the three baseline questions (see figure 3.1).



Figure 3.1 Baseline Questions for Module Selection Quiz

[Back to Home](#)

Module Selection

Reset All

Answer the following questions to determine the most appropriate VA module for your jurisdiction to use:

1	What is the known or perceived level of VA-related activities or operators in your jurisdiction?	<div></div>
2	Has your jurisdiction received international cooperation requests related to VAs, or are there suspicious transaction reports or investigations related to VAs?	<div></div>
3	Has your jurisdiction previously taken steps to understand the potential risks associated with VA and VASPs?	<div></div>

Further questions may appear depending on the answers to the baseline questions. Once all applicable questions have been answered, a recommendation will appear at the bottom of the tab (see figure 3.2).

The tool makes a recommendation by considering both the materiality of virtual assets in the jurisdiction and the capacity of the authorities and the depth of experience in assessing risk in this sector. For jurisdictions with limited VA activities and limited risk assessment experience, the quiz will recommend the basic module. Alternatively, the tool will encourage jurisdictions with higher VA materiality and experience in either reviewing risk or regulating the sector to consider a higher-tier module. Jurisdictions interested in seeing the underlying logic behind the quiz recommendations should refer to the decision tree in annex 1. All recommendations on the proposed tier are optional; the final decision on which module to use rests with the working group.



Figure 3.2 Example of Module Recommendation

Intermediate

Thank you for completing your survey. It is recommended that you use the Intermediate module.

Please return to the Home page and select the Intermediate module.

If once the working group has completed the survey the members wish to retake the quiz, they should use the “Reset All” button at the top of the tab. Table 3.1 provides additional guidance on each of the questions. Please note that the flow of the questionnaire is determined dynamically depending on the answers to the baseline questions. As a result, not all questions listed in table 3.1 may be visible in each case.

Table 3.1 Guidance to Module Quiz Questions

	Question	Guidance
Baseline questions	What is the known or perceived level of VA-related activities or operators in your jurisdiction?	<p>The working group should consider both known data and perceptions when answering this question. The potential levels have the following meaning:</p> <p>“High”: There are a material number of domestic VASPs or VA activities occurring locally, whether through regulated or unregulated channels, or both.</p> <p>“Medium”: VA use and VASP registrations are limited in the jurisdiction, but legal and/or illegal use of VAs is observed on a regular basis.</p> <p>“Low”: VAs use is almost nonexistent and there are no registered/licensed VASPs in the jurisdiction.</p> <p>“Unknown”: The working group has no information on the materiality of VA use or VASP activities.</p> <p>The working group may refer to the list of jurisdictions with materially important VASP activity published by the FATF in 2024 (see “Related FATF Documents” later in this guide).</p>
	Has your jurisdiction received international cooperation requests related to VAs, or are there suspicious transaction reports or investigations related to VAs?	<p>This question is designed to gauge the extent to which there are known or perceived threats facing VA and VASP activities in the jurisdiction. The potential levels have the following meaning:</p> <p>“Yes, many”: The jurisdiction has received a material number of international cooperation requests or there are suspicious transaction reports, investigations, or intelligence related to VA or VASP misuse. When deciding what a material number is, jurisdictions may wish to consider whether the number is proportionate when compared to the size of the local VA sector.</p> <p>“Yes, some”: The jurisdiction has received some international cooperation requests or has produced suspicious transaction reports, investigations, or intelligence related to VA or VASP misuse.</p> <p>“No”: The jurisdiction has not received any international cooperation requests related to VA or VASP misuse and does not have any ML/TF investigations related to VAs. The volume of STRs is extremely limited.</p>
	Has your jurisdiction previously taken steps to understand the potential risks associated with VA and VASPs?	<p>Potential answers: “yes”/“no”. When answering this question, jurisdictions should respond “yes” if they have taken any ad hoc steps to identify the risks of the sector. Such efforts need not have been done as part of a formal national risk assessment.</p>

Follow-up questions (as applicable)	<p><i>Depending on the answers to the baseline questions, a subset of follow-up questions will appear. The working group should answer all visible questions to obtain a recommendation on the suitable tier. Potential answers to follow-up questions: “yes”/“no”.</i></p>	
	Has your jurisdiction established a regulatory framework and appointed a competent authority to license and supervise VASPs?	The response to this question should consider whether legislation has been passed to regulate the sector for AML/CFT purposes and/or to appoint an AML/CFT supervisor.
	Is there evidence of domestic VASPs or financial institutions providing more complex VA-related services (such as interconnected VA services between VASPs and financial institutions, services across multiple VA activities and types, new or unregulated products)?	When deciding whether the local VA market is providing complex services, jurisdictions should consider the breadth of VA services being offered. For example, jurisdictions with only one local VASP which provides one type of service, to a limited local market may select “no”. Alternatively, jurisdictions with multiple local VA companies or evidence of locals accessing more complex services should select “yes”.
	Is there evidence of the local population accessing VA services outside of regulated providers (such as through illegal operators or decentralized peer-to-peer transactions ^a)?	To inform the response to this question, jurisdictions may wish to consult local VASPs, financial institutions, and/or open-source information from blockchain analytics companies to better understand the extent to which locals are accessing decentralized services.

Note: AML/CFT = anti-money laundering/countering the financing of terrorism; STRs = suspicious transaction reports.

a. The FATF defines peer-to-peer (P2P) transactions as VA transfers conducted without the use or involvement of a VASP or other obliged entity (such as VA transfers between two unhosted wallets whose users are acting on their own behalf). P2P transactions are not explicitly subject to AML/CFT controls under the FATF Standards. This is because the standards generally place obligations on intermediaries rather than on individuals themselves (with some exceptions, such as requirements related to implementing targeted financial sanctions).

Step 1.2. Qualitative Scoping and Mapping

Home tab

Once the working group has completed the Module Selection quiz, the working group should fill in the requested information in the “Home” tab, including inserting the jurisdiction’s name and desired module tier. The working group should make sure to select the appropriate module tier, drawing on any recommendation provided by the Module Selection Quiz.

If no module version is selected in the “Home” tab, the automatic default will be the advanced version.

The World Bank's risk assessment tool has been designed to support jurisdictions as they assess national risks. Jurisdictions with subnational regions (federal systems or provinces) may choose to use the tool to assess risks within specific provinces, where there is evidence that such risks differ. Finally, the "Home" tab also includes a checklist of suggested activities the working group should complete before advancing with the assessment, including ensuring that the working group is established and that members have read this guidance document.

Definitions tab

In order to inform the working group's decisions on scoping, all jurisdictions should complete the requested information under the "Definitions" tab. This is an important part of the scoping because it helps ensure that the working group members have a shared understanding of the terminology used. This section requests jurisdictions answer the following key questions:

- How are virtual assets defined under national law?
- How are virtual asset service providers (VASPs) defined under national law?
- Is the national definition of VAs and VASPs consistent with the FATF definitions (please refer to section 2.3 for additional guidance)?
- Beyond the general definitions provided, do you have any additional national definitions for specific VASP subsectors, services, or products? If so, please insert these definitions below.

For jurisdictions that indicate that they have gaps or deficiencies in their national definitions of VAs or VASPs, the tool will automatically take this into account when assessing the impact of AML/CFT mitigation measures.

After completing the "Home" and "Definitions" tabs, the working group should then move to the "General Mapping" tab. This step requires the working group to collect key contextual information to better understand the materiality and nature of VA use in the jurisdiction. This section includes questions on the sector's structure, key actors, regulatory frameworks, and relevant case studies that provide important context for later sections.

Much of the contextual information collected for this step is qualitative (such as text, descriptions, and explanations). While it does not directly affect the final risk ratings, this contextual information will serve as the basis for assessing indicators in subsequent steps (such as the threat, vulnerability, and mitigation analysis). Table 3.2 offers additional guidance on the questions.

Table 3.2. Additional Guidance on Mapping Questions

Tab	Questions	Guidance
General mapping	Materiality of virtual assets	
	Do you have any data on the volume of local consumers that use, access, or own virtual asset services (whether locally or abroad)? If yes, please specify.	<p>When answering this question, jurisdictions should consider the following primary and secondary data sources:</p> <p>Primary data sources</p> <ul style="list-style-type: none"> • Data from domestic and foreign VASPs on the number of local customers • Data from local financial institutions on the number of their clients conducting financial activities in VAs • Data from tax authorities on the volume of citizens reporting taxable virtual assets • Any surveys conducted by the central bank or other authorities to determine VA adoption within the jurisdiction <p>Secondary data sources</p> <ul style="list-style-type: none"> • Open-source information and market research reports from blockchain analytics companies on VA adoption by jurisdiction <p>Jurisdictions should use official data where possible and should indicate the source of any informal estimates.</p>
	What types of services are local consumers accessing? (multiple choice)	<p>When answering these open-text questions, jurisdictions should consider the following:</p> <p>Primary information sources</p> <ul style="list-style-type: none"> • Information from local and foreign VASPs on the (a) types and (b) volume of services that they provide to local clients • Information from traditional financial institutions on the types of VA types and activities that clients are engaging in • Information from domestic or foreign VASP supervisors about the scope of VA services offered in the jurisdiction • Information from the financial intelligence unit and/or tax authorities on the types of virtual assets that people are reporting on <p>Secondary information sources</p> <ul style="list-style-type: none"> • Market reports on volume and nature of VA adoption in the jurisdiction, and/or on use of decentralized services • Expert perceptions on the nature of VA adoption in the jurisdiction
	What types of virtual assets are local consumers buying, selling, trading, and so on?	
	To what extent are local consumers accessing VA services through domestic VASPs versus foreign VASPs?	
	To what extent are local consumers accessing VA services through centralized VASPs versus peer-to-peer ^a or decentralized financial services?	

General mapping	Domestic VASP ^b sector size and nature	
	How many locally licensed/registered VASPs do you have?	Please indicate the total number of VASPs registered in your jurisdiction for every year under review. The Excel tool will automatically update to show the previous four years from when the tool is being used. For jurisdictions that do not yet have a formal licensing/registration system, they may rely on approximative estimates.
	Are domestic VASPs licensed/registered and supervised for AML/CFT purposes?	Open text response. Please explain any applicable licensing or registration regimes.
	What services do domestic VASPs offer? Please name some of the domestic VASPs and the associated services they offer.	Information to respond to this question should come from supervisory data on any registered/licensed VASPs. The purpose of this question is to identify the services provided by VASPs in practice, which may be a subset of the ones permitted. This helps the working group assess the specific ML/TF risks associated with each service that is assessed in subsequent tabs.
	What VA-related services are (a) regulated under your legislation, (b) expressly prohibited, or (c) partially prohibited?	<p>To answer this question, the working group should gather information from tax authorities, as well as supervisory or central bank authorities responsible for financial stability and consumer protection regulation.</p> <p>When answering this question, the working group should consider applicable guidance and standards issued by international bodies, including the FSB High-Level Recommendations for the Regulation, Supervision and Oversight of Crypto-asset Activities and Markets,^c the FSB High-Level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements,^d the Guidance on Prudential Treatment of Cryptoasset Exposures published by the Basel Committee on Banking Supervision,^e the IOSCO Policy Recommendations for Crypto and Digital Asset Markets,^f the OECD's Crypto-Asset Reporting Framework,^g or the IMF-FSB Synthesis Paper on Policies for Crypto-Assets.^h Even jurisdictions that prohibit VA activities need to conduct a full ML/TF risk assessment of the sector.</p>

General mapping	Unlicensed/unregistered domestic VASPs and peer-to-peer services^a	
	What information do you have on the volume of unlicensed/unregistered domestic VASP activity and use of peer-to-peer platforms?	Information to answer these open-text questions should come from the following: Primary information sources <ul style="list-style-type: none"> • Data from law enforcement, the financial intelligence unit, or supervisor on detection of unlicensed/unregistered VA activity • Data from registered/licensed VASPs on the presence and scope of unregulated activity
	Are you proactively looking for local unlicensed/unregistered VASP or peer-to-peer activity? If so, please explain how.	Secondary information sources <ul style="list-style-type: none"> • Market research reports and data from blockchain analytics companies on unregulated/unlicensed VA activity
	Foreign VASP^b sector size/nature	
		<p>Understanding the use of foreign VA services that are not licensed in the jurisdiction is key for a comprehensive risk assessment. The VASPs in question may or may not be registered in another jurisdiction.</p> <p>To respond to this question, jurisdictions can consult the following:</p> <p>Primary data sources</p> <ul style="list-style-type: none"> • Information from domestic VASPs on the extent to which local clients are accessing foreign VASP services • Information from traditional financial institutions, such as banks, on the types of foreign VA services which clients are accessing (if known) • Secondary data sources • Open-source research on foreign VASPs that are pursuing targeted advertising for the local market • Market research on top VA exchangers by jurisdiction (for example, country reports from Cointelegraph and CoinMarketCap) <p>For this question, jurisdictions may also want to consider information received in compliance with the OECD's Crypto Asset Reporting Framework on the exchange of tax information. When assessing questions related to foreign VASPs, the working group should bear in mind that VASPs may regularly change the location of their headquarters and even their name.</p>

General mapping	Provision of VA services by non-VASPs	
	Do any other financial institutions or designated nonfinancial services or businesses (DNFBPs) provide services in VAs? If so, which ones?	Information to respond to these open-text questions should come from the following: Primary data sources <ul style="list-style-type: none"> • Information from financial and DNFBP supervisors on the extent to which obliged entities are providing services involving VAs • Information from financial institutions and DNFBPs on the provision of any services involving VAs • Information from the financial supervisor and central bank on the extent to which wider commercial merchants (such as retail shops) are accepting payment in VAs
	Do any local merchants accept payment via virtual assets? If so, which ones and how many?	Secondary data sources <ul style="list-style-type: none"> • Open-source search on any financial institutions, DNFBPs, or merchants that are accepting VA services or payments

Note: DNFBP = designated nonfinancial business and profession; FSB = Financial Stability Board; IOSCO = International Organization of Securities Commissions; OECD = Organisation for Economic Co-operation and Development.

a. The FATF defines peer-to-peer (P2P) transactions as VA transfers conducted without the use or involvement of a VASP or other obliged entity (such as VA transfers between two unhosted wallets whose users are acting on their own behalf). P2P transactions are not explicitly subject to AML/CFT controls under the FATF Standards. This is because the standards generally place obligations on intermediaries rather than on individuals themselves (with some exceptions, such as requirements related to implementing targeted financial sanctions).

b. Please refer to chapter 1 of this document for definitions of Domestic VASP and Foreign VASP with a material local presence.

c. Financial Stability Board, "High-Level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report," (Financial Stability Board, July 17, 2023), https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/?utm_source=chatgpt.com.

d. Financial Stability Board, "High-Level Recommendations."

e. Basel Committee on Banking Supervision, "Prudential Treatment of Cryptoasset Exposures" (Bank for International Settlements, December 2022), <https://www.bis.org/bcbs/publ/d545.pdf>.

f. Board of the International Organization of Securities Commissions, "Policy Recommendations for Crypto and Digital Asset Markets: Final Report" (Report FR11/2023, International Organization of Securities Commissions, November 16, 2023), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf>.

g. Organisation for Economic Co-operation and Development, International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 Update to the Common Reporting Standard" (OECD Publishing, 2023), https://www.oecd.org/en/publications/international-standards-for-automatic-exchange-of-information-in-tax-matters_896d79d1-en.html.

h. Financial Stability Board, "IMF-FSB Synthesis Paper: Policies for Crypto-Assets" (Financial Stability Board and the International Monetary Fund, September 7, 2023), <https://www.fsb.org/2023/09/imf-fsb-synthesis-paper-policies-for-crypto-assets/>.

Step 1.3. Quantitative Scoping and Mapping

For the final substep of the mapping, jurisdictions should gather quantitative data and any available case studies on VA misuse to inform their understanding of the ML/TF risks.

Data inventory

Specifically, under the “General Mapping” tab, jurisdictions should insert the following data for the period of the assessment:

- Data on the total number of predicate offenses in the jurisdiction [To narrow down this exercise, the tool requests only data for predicate offenses that globally are more susceptible to laundering and that involve virtual assets.]
- Data on the number and value of suspicious transaction reports related to VAs
- Data on the number of financial intelligence disseminations from the FIU on VAs
- Data on the number of money laundering investigations, prosecutions, and convictions related to VAs
- Data on the number of formal and informal cooperation requests sent and received related to virtual assets
- Data on the value of virtual assets seized and confiscated by the jurisdiction

Using the data inserted, the Excel tool then generates several analytical graphs to help jurisdictions interpret the data (see output 2 in section 4.2).

Under the “Case Studies” tab, jurisdictions should compile and summarize the facts of any known ML/TF investigations related to virtual assets. The objective of this exercise is to help jurisdictions review how ML/TF risks are manifesting in practice, including the key ML/TF techniques or VASP services being misused. The volume of cases which should be inserted will depend on the jurisdiction’s context, but at a minimum, jurisdictions should seek to gather information on at least three cases. Jurisdictions that do not have any domestic investigations involving virtual assets should gather the requested information for any prominent regional or global cases that appear relevant for the jurisdiction’s own domestic context.

Specifically, jurisdictions should gather the following information on the case studies:

- Brief account of the case (facts of the case)
- Crime(s) committed
- Total value of laundered assets
- VA type and VASP activity involved in the case
- Other sectors involved
- Origin and destination of illicit funds
- Result of the police investigation
- Conviction, penalty, asset forfeiture, or other action taken.

Step 1.4. (for advanced version only) Detailed VA and VASP Mapping Exercise

For jurisdictions that select the advanced module, two additional tabs will be visible (the “Entity Mapping” tab and the “VA Mapping” tab). Both exercises are optional and are intended to provide higher-capacity jurisdictions with additional information to inform their supervisory outreach and law enforcement efforts. The inputs provided for these mapping exercises are for reference only and are intended to help jurisdictions form their more detailed assessment of VA and VASP risk (assessed under step 5).

Entity Mapping (optional). For this tab, jurisdictions are invited to identify a representative sample of VASPs operating in their jurisdiction, including domestic VASPs and foreign VASPs that have a material local presence. This sample includes the following information: (a) registration data, (b) VASP activities and services, (c) fit and proper checks, (c) AML/CFT systems and controls, and (e) foreign exposure. The objective of this exercise is to help supervisors gather additional insights into VA companies operating locally.

VA Mapping (optional). Certain VA types pose higher inherent ML/TF vulnerabilities due to built-in features which facilitate privacy and speed. For this tab, jurisdictions are invited to identify examples of different types or categories of virtual assets held or in use in their jurisdiction, including virtual assets held in both custodial wallets and unhosted wallets. This input includes information on the following: (a) the prevalence of the virtual asset type, (b) the applicable regulation for this particular virtual asset (if distinct), and (c) the extent to which the virtual asset types have been connected to known ML/TF or other criminal activity. When conducting this assessment, jurisdictions could consider gathering information on emerging types of virtual assets, including any platform-issued tokens or governance tokens when used for payment or investment purposes.

3.2. Step 2: ML and TF Threat Assessment

Step 2 of the World Bank’s VA risk assessment tool helps jurisdictions assess the ML/TF threats facing the virtual asset sector (box 3.1). Given that jurisdictions may face a high exposure to ML, but not TF, or vice versa, the World Bank’s threat assessment on VAs distinguishes between ML and TF.



Box 3.1. What is a threat in the context of VAs?

In the context of virtual assets, a money laundering or terrorist financing threat refers to individuals, groups, entities, or their facilitators who seek to exploit virtual assets (VAs) or related services to conceal the illicit origin of funds or to finance terrorism. Examples include the following:

- An organized crime group generating cash proceeds and converting them into VAs to hide their illicit origin
- A cybercriminal who extorts victims online, generating proceeds in virtual assets
- Individuals soliciting donations in virtual assets to support terrorist fighters in another jurisdiction

This step comprises two substeps: (a) an assessment of national ML/TF threats and (b) a typologies assessment. Additional guidance on both steps follows. Typically, law enforcement, intelligence agencies, and the FIU will need to play a key role in generating insights to inform this part of the assessment.

National ML and TF Threats

The “National ML and TF Threats” tab requires jurisdictions to assign ratings to key threat variables and to conduct a qualitative assessment on the nature of the ML/TF threats. For this assessment, jurisdictions are required to reflect on the geographic dimension of the threat (such as whether ML/TF threats are internal, incoming, outgoing, or a combination of these) and whether threats are known or perceived. Box 3.2 provides additional guidance on the definitions of these terms and table 3.3 offers guidance on completing the tab.



Box 3.2. Guidance on Key Threat Terms

Internal ML/TF threat. Internal money laundering/terrorist financing (ML/TF) threats are criminal proceeds or terrorist funds that are generated in the jurisdiction and are then laundered domestically or used to finance terrorism domestically via virtual asset (VA) activities or virtual asset service providers (VASPs) in the jurisdiction.

Incoming ML/TF threat. Incoming threats are criminal proceeds or terrorist funds that are generated overseas and then enter the jurisdiction to be laundered or spent via VA activities or VASPs in the jurisdiction.

Outgoing ML/TF threat. Outgoing threats are criminal proceeds or terrorist funds that are generated in the jurisdiction and are then transferred abroad to be laundered via VAs or VASP activities overseas.

Perceived versus known-level of threat. The known level of ML/TF threat should be based on concrete investigations, prosecutions, convictions, or other forms of concrete intelligence (such as supervisory findings or financial intelligence unit disseminations). The perceived level may rely on expert opinions or credible open-source data.

Table 3.3, Guidance on Completing the “ML/TF Threats” Tab

Topic	Variable description	Potential assessment ratings	Guidance
General national ML and TF threats (non-VA specific)	1. National money laundering threat level	Very high, high, medium-high, medium. Medium-low, low, very low.	<p>To complete these questions, jurisdictions should refer to the general ML/TF threat level identified during the last national risk assessment. Notably, this rating should be the general threat level and not the specific threat facing the VA sector (which is assessed separately at a later stage).</p> <p>If there is evidence that the threat picture has changed significantly since the last national risk assessment, the working group may choose to select a different rating than that assigned during the last NRA.</p>
	2. National terrorist financing threat level		
Analysis of exposure of VASPs to the threat of money laundering	<p><i>Internal/incoming ML threat involving use of virtual assets</i></p> <p>3. Data known to law enforcement authorities on use of VAs in national ML investigations, prosecutions or convictions or predicate offenses</p> <p>4. Perceived level of internal/incoming ML threat, based on</p> <ul style="list-style-type: none"> Open and reliable sources of information Expert opinion 	Very high, high, medium-high, medium. Medium-low, low, very low, not applicable, unknown.	<p>When assessing these indicators jurisdictions should consider the following:</p> <p>Data sources for known threats</p> <ul style="list-style-type: none"> Law enforcement data on the number of known ML or predicate investigations, prosecutions, and convictions in the jurisdiction involving VAs Other forms of concrete intelligence (supervisory findings or FIU disseminations) Data sources for perceived level of threats Credible open-source data (such as available data from industry representatives). This could include any estimates on the percentage of the local market involving criminal transactions. Law enforcement and private sector expert opinions on the level of internal or incoming criminal threats facing the local VA sector <p>These questions focus on the internal and incoming criminal threat facing domestic VASPs.</p>

Analysis of exposure of VASPs to the threat of money laundering	<p>Outgoing ML threat involving use of virtual assets</p> <p>5. Data known to law enforcement authorities on foreign ML investigations, prosecutions, or convictions involving VAs with links to your jurisdiction</p> <p>6. Perceived level of outgoing ML threats involving use of virtual assets, based on</p> <ul style="list-style-type: none"> • Open and reliable sources of information • Expert opinion 	<p>Very high, high, medium-high, medium. Medium-low, low, very low, not applicable, unknown.</p>	<p>When assessing these indicators jurisdictions should consider the following:</p> <p>Data sources for known threats</p> <ul style="list-style-type: none"> • International cooperation requests or other forms of foreign intelligence on ML occurring overseas, involving VAs • Data on any joint investigations involving domestic predicate offenses, with laundering in VAs overseas • Data sources for perceived level of threats • Credible open-source data indicating whether criminal proceeds are moved overseas to be laundered through foreign VASPs or unregulated channels • Law enforcement and private sector expert opinions on the level of outgoing criminal threats <p>If the jurisdiction has no cooperation with foreign counterparts on VAs and limited cooperation on ML, the working group should consider applying a rating of “unknown”.</p>
Analysis of exposure of VASPs to the threat of terrorist financing	<p><i>Internal/incoming TF threat involving use of virtual assets</i></p> <p>7. Data known to law enforcement authorities on use of VAs in national TF investigations, prosecutions, or convictions</p> <p>8. Perceived level of the internal/incoming TF threat involving use of virtual assets, based on</p> <ul style="list-style-type: none"> • Open and reliable sources of information • Expert opinion 	<p>Very high, high, medium-high, medium. Medium-low, low, very low, not applicable, unknown.</p>	<p>These questions focus on the movement and use of VAs by terrorist groups operating within the jurisdiction.</p> <p>When assessing these indicators jurisdictions should consider the following:</p> <p>Data sources for known threats</p> <ul style="list-style-type: none"> • Law enforcement data on the number of known terrorism or TF investigations, prosecutions, and convictions in the jurisdiction involving VAs • Other forms of concrete intelligence on TF through domestic VA activities and VASP sector (supervisory findings or FIU disseminations) • Data sources for perceived level of threats • Credible open-source data (such as available data from industry representatives) on the level of TF threat for domestic VASPs and VA activities • Law enforcement and private sector expert opinions on the level of internal or incoming terrorist threats facing the local VA sector

Analysis of exposure of VASPs to the threat of terrorist financing	<p><i>Outgoing TF threat involving use of virtual assets</i></p> <p>9. Data known to law enforcement authorities on foreign TF investigations, prosecutions, or convictions involving VAs with links to the jurisdiction</p> <p>10. Perceived level of outgoing TF threat involving use of virtual assets, based on</p> <ul style="list-style-type: none"> • Open and reliable sources of information • Expert opinion 	<p>Very high, high, medium-high, medium. Medium-low, low, very low, not applicable, unknown.</p>	<p>These questions focus on the threat of funds being used to finance terrorist groups or actors operating overseas.</p> <p>Data sources for known threats:</p> <ul style="list-style-type: none"> • International cooperation requests or other forms of foreign intelligence on VA donors for TF occurring overseas • Data on any joint investigations involving local donations for TF in VAs <p>Data sources for perceived level of threats:</p> <ul style="list-style-type: none"> • Credible open-source data indicating whether virtual assets are being moved overseas to fund terrorist activities • Law enforcement and private sector expert opinions on the level of outgoing terrorist financing threats <p>If the jurisdiction has no cooperation with foreign counterparts on VAs and limited cooperation on TF, the working group should consider applying a rating of “unknown”.</p>
Qualitative analysis—money laundering threats	<p>11. Which are the foreign jurisdictions mostly involved in ML cases in which VAs have been involved?</p> <p>12. Which types of criminal actors are known or believed to use VAs?</p> <p>13. Based on investigations, what is the prevalence of use of obfuscation measures (darknet use, illicit use of mixers, exchanges with no KYC, and so on) in criminal cases?</p> <p>14. Which types of predicate offenses are most commonly linked to ML in your jurisdiction?</p> <p>15. What is the proportion of ML cases involving tax crimes where VAs are used?</p>	<p>Qualitative open-text response.</p>	<p>When responding to these questions, jurisdictions should consider the following:</p> <ul style="list-style-type: none"> • Details of any ML cases or STRs involving virtual assets • Information from law environment and intelligence authorities on prevalence of darknet use <p>When answering question 11, the working group should identify material foreign jurisdictions that are involved in any stage of the laundering cycle (including where the predicate takes place, where the VASP is located, and so on).</p> <p>For question 12, different types of actors may include professional money launderers, self-launderers, organized crime groups, individuals selling illicit goods, and so on.</p> <p>Working groups should distinguish in the answers between known data based on investigations and the perceived level of use based on expert opinion and open-source data.</p>

Qualitative analysis—terrorist financing threats	<ul style="list-style-type: none"> 16. Which are the foreign jurisdictions mostly involved in TF cases in which VAs have been involved? 	Qualitative open-text response.	<p>When responding to these questions, jurisdictions should consider the following:</p> <ul style="list-style-type: none"> Information on TF cases, or intelligence involving virtual assets <p>When answering question 16, the working group should identify material foreign jurisdictions that are involved in any stage of the TF cycle (such as any prominent jurisdictions where funds are raised, moved, or spent). For question 17, types of actors may include terrorist groups of different size and ideology, lone wolves, and so on.</p> <p>Working groups should distinguish between known data based on investigations and the perceived level of use based on expert opinion and open-source data.</p>
	<ul style="list-style-type: none"> 17. Which types of terrorist actors are known or believed to use VAs? 		

Note: FIU = financial intelligence unit; KYC = know your customer; NRA = national risk assessment.

ML and TF Techniques

In the second and final part of the threat assessment, jurisdictions undertake a typologies assessment. For this exercise, jurisdictions should review the list of ML and TF techniques included in the relevant Excel tab and should assign a rating for the level of known and perceived prevalence (see additional guidance in table 3.4). The objective of this exercise is to help jurisdictions understand how risk is manifesting in practice to help inform outreach to the VA sector.

The World Bank team has identified these techniques using an in-depth review of case studies and global typologies reports. For a full list of the typologies, alongside the descriptions and source documents, see annex 2. For jurisdictions that select the intermediate and advanced modules, there are progressively more techniques to assess, reflecting the evolving sophistication as service and products develop. In addition to techniques identified in annex 2, the Excel tool also provides flexibility for jurisdictions to identify any additional techniques which may be relevant for the jurisdiction.

Known ML and TF techniques involving VAs have been grouped into four categories:

- Traditional obfuscation techniques** that criminals and terrorist actors have adapted for the VA sector. These techniques mirror similar techniques seen in traditional finance (such as mule accounts and structuring).
- New obfuscation techniques** that rely on unique characteristics of VA and distributed ledger technology—that is, techniques that do not have a direct equivalent in traditional finance.
- Techniques used specifically for generating criminal proceeds in virtual assets.**
- Techniques specific to terrorist financing.**

Using the responses for this section, the World Bank tool automatically generates a prioritization of techniques to help inform the authorities outreach to the private sector (see output 3 in chapter 4).

Table 3.4 Additional Guidance on Assessing ML/TF Techniques.

Variable description	Potential assessment ratings	Guidance
ML and TF techniques	Evaluation Comments on characteristics of the technique in the jurisdiction	<p>For each technique the working group should rate the prevalence based on (a) known data and (b) expert opinion/perception. Potential ratings: very high, high, medium high, medium, medium-low, low, very low, unknown. Information sources which should be considered include the following:</p> <p>For known data</p> <ul style="list-style-type: none"> Concrete evidence that the technique has occurred in the jurisdiction (based on known ML/TF or predicate investigations, or STRs) <p>For expert perception/opinion</p> <ul style="list-style-type: none"> Suspicion that the technique may have occurred or is likely to occur in the future based on expert judgment and open-source information <p>If the working group does not have sufficient information to make an assessment, it should select the “unknown” option.</p> <p>Jurisdictions should use this column to justify their assigned rating, and specifically should cite any specific cases or data sources that informed the judgment.</p>
	Add more typologies as appropriate	The final row in the Excel table provides an option for jurisdictions to add additional techniques as appropriate. This flexibility is important given that techniques are regularly evolving.

3.3. Step 3: National Vulnerabilities

Step 3 of the World Bank's VA risk assessment tool helps jurisdictions to assess the ML/TF vulnerabilities related to the misuse of VAs and VASPs (box 3.3).



Box 3.3 What is a ML/TF vulnerability in the context of VAs?

Vulnerabilities refer to factors that make a jurisdiction, a sector, or a particular service attractive for money laundering (ML) or terrorist financing (TF), and which can be exploited by threat actors. Vulnerabilities can be both inherent features of a service or jurisdiction (such as its geographic location or proximity to terrorist threats) or vulnerabilities caused by specific gaps in country capacity (such as deficiencies in supervisory capacity). In the context of virtual assets, some examples of vulnerabilities include the following:

- Domestic virtual assets service providers (VASPs) offering services to a large number of high-risk clients (such as politically exposed persons or foreign clients from high-risk jurisdictions).
- Systemic deficiencies with local identity infrastructure which presents challenges for effective customer due diligence when VASPs onboard new clients.

Step 3 of the World Bank's VA risk assessment tool includes a consideration of three types of vulnerability:

- **General vulnerabilities arising from the jurisdiction's wider context**—including the strength of the jurisdiction's identity infrastructure and transparency around company ownership. The World Bank's VA risk assessment tool recognizes that such wider contextual factors will have an impact on the extent to which all sectors, including virtual assets, are vulnerable to misuse.²²
- **Vulnerabilities that are inherent to the local VASP sector.**
- **Vulnerabilities that are inherent to foreign VASPs operating in the jurisdiction.**

See table 3.5 for detailed guidance on how to evaluate each of these vulnerabilities.

Table 3.5. Additional Guidance on Assessing ML/TF Vulnerabilities

Topic	Variable description	Assessment ratings	Guidance
General national inherent vulnerabilities	1. Extent to which the jurisdiction is an international or regional finance and/or company formation center	Very high, high, medium-high, medium, medium-low, low, very low	<p>A jurisdiction's status as an international or regional finance and/or company formation center increases the volumes of incoming financial flows, which, depending on the origin and nature of flows, may increase the ML threat and vulnerability level. When deciding the appropriate rating for this indicator jurisdictions may wish to consider the following:</p> <ul style="list-style-type: none"> • The concentration of financial institutions and the provision of specialized financial services • The volume of cross-border transactions. • The volume of companies established under local laws, in comparison to the size of the domestic population (see for example, World Bank's entrepreneurship database).
General national inherent vulnerabilities	2. Limitations to transparency and accessibility of beneficial ownership information at the jurisdiction level	Very high, high, medium-high, medium, medium-low, low, very low	<p>Opacity of company ownership data can make a jurisdiction more attractive for criminals to launder funds and finance terrorism.</p> <p>When deciding the appropriate rating, jurisdictions should consult the following sources: the jurisdiction's latest FATF assessment on Recommendations 24 and 25 (R.24 and R.25) and Immediate Outcome 5, and the OECD Global Forum assessments.</p> <p>Jurisdictions with noncompliant or partially compliant ratings for FATF's R.24 or 25, should not rate this variable as lower than "medium".</p>
	3. Limitations to reliable identification of natural persons at the jurisdiction level	Very high, high, medium-high, medium, medium-low, low, very low	<p>Authorities should consider the percentage of the population that has access to a formal ID or another form of government-approved identification. The lack of formal identification may limit the effectiveness of preventive measures taken by obliged entities and therefore contribute to vulnerabilities for ML and TF.</p>

General national inherent vulnerabilities	4. Prevalence of use of cash across the jurisdiction	Very high, high, medium-high, medium, medium-low, low, very low	<p>A high use of cash within the jurisdiction can reduce the traceability of financial flows and contribute to a jurisdiction's vulnerability for ML and TF.</p> <p>When deciding the rating for this variable, jurisdictions should consider the following:</p> <ul style="list-style-type: none"> • Data from the central bank data on money circulation • Consumer surveys on use of cash • Data on financial inclusion (such as the World Bank Global Findex database) or the ratio of bank assets to GDP. <p>Generally, the lower the use of the formal financial sector, the higher the likelihood of financial flows occurring in cash.</p>
	5. Extent of corruption in the jurisdiction	Very high, high, medium-high, medium, medium-low, low, very low	<p>Corruption is not only a predicate crime for ML, but also a factor potentially undermining AML efforts, thereby creating vulnerabilities. When answering this question, the working group should focus on corruption affecting AML efforts.</p> <p>When deciding the rating, jurisdictions should consider the following:</p> <ul style="list-style-type: none"> • Data from national anticorruption agency or law enforcement • Reports by other relevant regional or global bodies (such as under the United Nations Convention Against Corruption) • Transparency
	7. Overall level of delivery of VA services	Very high materiality, high materiality, medium-high materiality, medium materiality, medium-low materiality, low materiality, very low materiality	<p>The different VA activity types for this question align with both the FATF definition of a VASP and the subsequent taxonomy provided by step 5 of the World Bank's tool (the VASP assessment). When determining the materiality of different service types, the working group may wish to consult the following:</p> <p>Primary data sources</p> <ul style="list-style-type: none"> • Data provided by domestic VASPs on the nature and volume of their services • Supervisory data on the materiality of different types of VA services <p>Secondary data sources</p> <ul style="list-style-type: none"> • Open-source data on the scale and importance of different services being offered by VASPs in the jurisdiction

General national inherent vulnerabilities	8. Risk profile of the domestic VASP client base	Very high risk, high risk, medium-high risk, medium risk, medium-low risk, low risk. Very high vulnerability, high vulnerability, medium-high vulnerability, medium vulnerability, medium-low vulnerability, low vulnerability, very low vulnerability.	<p>The working group should assess the extent to which domestic VASPs are onboarding and servicing high-risk clients. High-risk clients may include the following:</p> <ul style="list-style-type: none"> Politically exposed persons Foreign clients from high-risk jurisdictions for ML/TF or sanctions evasion Customers known via publicly available information to law enforcement due to previous criminal association <p>Information on the customer base should be obtained from supervisory data or direct engagement with VASPs, and supplemented by open-source data.</p>
	9. Extent to which domestic VASPs offer services with enhanced anonymity (services involving privacy coins and/or mixers tumblers)	Very high vulnerability, high vulnerability, medium-high vulnerability, medium vulnerability, medium-low vulnerability, low vulnerability, very low vulnerability	<p>Services with enhanced anonymity might include the following:</p> <ul style="list-style-type: none"> VASPs offering services with weak customer onboarding checks Services involving privacy coins (including. Monero and Zcash) Decentralized services (based on smart contracts) Use of mixers or tumblers <p>Answers to this question should rely on a combination of the following: intelligence, investigations, supervisory data, or engagement with domestic VASPs.</p>
	10. Prevalence of the use of cash in the domestic VASP sector	Very high vulnerability, high vulnerability, medium-high vulnerability, medium vulnerability, medium-low vulnerability, low vulnerability, very low vulnerability	<p>Answers for this question should consider the following:</p> <p>Primary data sources</p> <ul style="list-style-type: none"> Data from domestic VASPs on the prevalence of use of cash by clients when making trades Data from VASP supervisory outreach on the prevalence of the use of cash <p>Secondary data sources</p> <ul style="list-style-type: none"> Data from the central bank on use of cash generally in the economy (very high use of cash locally will increase the chances that the VASP sector is also exposed to cash) Presence of local VA ATMs (which may increase the options for cash deposits and withdrawals)

General national inherent vulnerabilities	11. Extent to which locals are accessing domestic decentralized services	Very high vulnerability, high vulnerability, medium-high vulnerability, medium vulnerability, medium-low vulnerability, low vulnerability, very low vulnerability	<p>For the purpose of this question, decentralized services may include the following</p> <ul style="list-style-type: none"> • Peer-to-peer transactions • Financial activities on decentralized platforms (such as decentralized exchangers or lending platforms which run on smart contracts) <p>Information to inform the response to this question may come from the following:</p> <ul style="list-style-type: none"> • Data or perceptions from domestic VASPs or other industry representatives • Information from the FIU, law enforcement, and supervisory data
Inherent vulnerability of foreign VASPs with material local presence^a	12. Overall size/turnover of foreign VASPs with material local presence/customer base	Very high materiality, high materiality, medium-high materiality, medium materiality, medium-low materiality, low materiality, very low materiality.	<p>When assessing this variable, jurisdictions should consider the following:</p> <p>Primary sources</p> <ul style="list-style-type: none"> • Information from foreign supervisors about the size/turnover of foreign VASPs with a material local presence • Information from foreign VASPs themselves about their turnover <p>Secondary sources</p> <ul style="list-style-type: none"> • Open-source data on the materiality of foreign VASPs with a material local presence (see for example CoinMarketCap for information on specific exchangers)
	13. Quality of data and intelligence on the local presence of foreign VASPs	Very high quality, high quality, medium-high quality, medium quality, medium-low quality, low quality, very low quality	<p>When determining the rating for this variable, jurisdictions should consider the following:</p> <ul style="list-style-type: none"> • The depth of international cooperation with foreign counterparts on VASP supervision • The scale of information gaps on foreign VASPs operating locally

Inherent vulnerability of foreign VASPs with material local presence^a	14. Overall level of delivery of VA services	Very high materiality, high materiality, medium-high materiality, medium materiality, medium-low materiality, low materiality, very low materiality	<p>When rating this variable, jurisdictions may consider the following:</p> <p>Primary data sources</p> <ul style="list-style-type: none"> • Data provided by foreign VASPs on the nature and volume of their services • Data from foreign supervisors on the materiality of different types of services offered by foreign VASPs with a material local presence <p>Secondary data sources</p> <ul style="list-style-type: none"> • Open-source data on the scale and importance of different services being offered by material foreign VASPs operating in the jurisdiction
	15. Risk profile of foreign VASPs with material local presence/ customer base	Very high vulnerability, high vulnerability, medium-high vulnerability, medium vulnerability, medium-low vulnerability, low vulnerability, very low vulnerability	See guidance in question 8 for examples of high-risk customers. The responses to these questions should rely on a combination of the following: information from foreign supervisors, information from foreign VASPs themselves, and open-source information gathering.
	16. Extent to which foreign VASPs with a material local presence are offering services with enhanced anonymity	Very high vulnerability, high vulnerability, medium-high vulnerability, medium vulnerability, medium-low vulnerability, low vulnerability, very low vulnerability	See guidance in question 9 for examples of anonymity-enhancing services. The response to this question should rely on a combination of the following: information from foreign supervisors, information from foreign VASPs themselves, and open-source information gathering.

Note: GDP = gross national product.

a. As mentioned in chapter 1, a material local presence may be defined as those VASPs that have a significant local customer base and/or that target their advertising for the local market

3.4. Step 4: National Mitigation Measures

The fourth step of the World Bank VA risk assessment tool is an assessment of the strength of existing mitigation measures against misuse of VAs and VASPs in the jurisdiction. This step requires jurisdictions to consider both the legislative controls in place (that is, technical compliance) as well as the effectiveness of such controls in practice. To complete this step, jurisdictions should review the variables in the “National Mitigation Measures” tab and assign assessment ratings. For detailed guidance on how to assess the different variables see table 3.6.

>>>

Table 3.6 Additional Guidance on Assessing National Mitigation Measures

Topic	Variable description	Assessment ratings	Guidance
Technical compliance with FATF’s Recommendation 15	Country compliance with FATF’s criterion 15.3–15.11	C—compliant LC—largely compliant PC—partially compliant NC—noncompliant	These questions are mapped to the FATF methodology for assessing technical compliance. The working group can refer to recent mutual evaluation reports, follow-up reports, or other assessments. However, the responses should reflect any legal or regulatory developments that have occurred in the meantime.
Effectiveness of implementation of AML/CFT preventive measures by domestic VASPs	10. Risk assessment and mitigation	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	To complete these questions, the working group will need to gather information on the practical effectiveness of AML/CFT controls by domestic VASPs. Jurisdictions may wish to refer to any recent FATF effectiveness ratings for Immediate Outcomes 1, 3, 4, or 6 (as relevant). A rating of “very high” or “high” for these areas suggests that the domestic VASPs are demonstrating high and substantial levels of effectiveness (as per FATF ratings). Jurisdictions that do not have any regulatory requirements or a supervisory system for VASPs should respond “not applicable”.
	11. Customer identification and due diligence		
	12. Enhanced measures for higher-risk situations		
	13. Travel Rule implementation		
	14. Suspicious transaction reporting and monitoring		

Effectiveness of implementation of AML/CFT preventive measures by foreign VASPs with material local presence^a	15. Risk assessment and mitigation	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>To complete these questions, the working group will need to gather information on the practical effectiveness of AML/CFT controls by foreign VASPs with a material local presence.</p> <p>For this, jurisdictions should refer to the following:</p> <ul style="list-style-type: none"> • Information obtained from foreign supervisors • Information obtained from open-source checks on the comprehensiveness of AML/CFT controls by foreign VASPs • Information obtained from FATF reports on the effectiveness of VASP preventive measures in the home supervisor jurisdiction <p>Jurisdictions that are unable to obtain any information should indicate “unknown”.</p>
	16. Customer identification and due diligence		
	17. Enhanced measures for higher-risk situations		
	18. Travel Rule implementation		
	19. Suspicious transaction reporting and monitoring		
Other	20. Effectiveness of local AML/CFT entry controls and enforcement for VASPs, including the ability of supervisors to detect and disrupt illegal VASP operators	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>When responding, jurisdictions should consider the ability of supervisors to (a) prevent criminals and their associates from controlling or being the beneficial owner of VASP activities, and to (b) detect and disrupt illegal VASP operators.</p> <p>Relevant data sources may include the following:</p> <ul style="list-style-type: none"> • Information on the comprehensiveness of fit and proper checks for VASPs (such as including the extent to which the jurisdiction has rejected any VASP applications for AML/CFT related reasons) • Evidence of successful detection and sanctioning of unlicensed activity in practice • Data from the FIU or domestic VASPs on the prevalence of unlicensed VASP activity • Strength of current detection tools (whistleblower regimes and/web scrapping) <p>When deciding on the rating for this variable, jurisdictions may also wish to refer to any recent FATF ratings for criterion 15.4 and 15.5.</p> <p>Jurisdictions with no supervisory framework will likely score as low or very low.</p>

Other	21. Effectiveness of risk-based supervision of domestic VASPs	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>When scoring this variable, jurisdictions should consider the following:</p> <ul style="list-style-type: none"> The adequacy of supervisory resources and knowledge for VASP supervision Whether the jurisdiction has started taking enforcement actions in practice <p>Jurisdictions that have not yet started conducting inspections of VASPs should rate this variable as “medium-low”, “low”, or “very low”.</p>
	22. Effectiveness of law enforcement capacity to detect and investigate ML or TF cases involving VAs	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>When deciding on the rating, jurisdictions should consider the following:</p> <ul style="list-style-type: none"> The quality/volume of local suspicious transaction reporting on VA activities (low volume may suggest oversight for detection) The adequacy of investigative resources and expertise to pursue VA cases The number of ML/TF investigations and prosecutions related to VAs which have been opened (and whether this is proportionate when considering the size of the local VA market)
	23. National capacity to conduct blockchain analytics in ML and TF cases involving VAs	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>Jurisdictions should consider the following:</p> <ul style="list-style-type: none"> The capacity of law enforcement and supervisors to use blockchain analytics tools to add value to their work <p>This rating should consider both the access to relevant tools and the internal capacity to use such tools.</p>
	24. Effectiveness of international cooperation and information sharing with foreign counterparts on VASPs	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>Jurisdictions should consider the following:</p> <ul style="list-style-type: none"> The extent to which national authorities are coordinating and cooperating with foreign counterparts on VA and VASP issues The existence of information gaps on foreign VASPs operating locally
	25. Effectiveness of regulations or guidelines to clarify tax requirements for VAs/ VASPs	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>Jurisdictions should consider the following:</p> <ul style="list-style-type: none"> Legislation on new VA-related taxable events Guidance to support compliance when traditional taxable events involve VAs Tax guidance concerning the treatment of VA-related services (such as wallet services)

a. As mentioned in chapter 1, a material local presence may be defined as those VASPs that have a significant local customer base and/or that target their advertising for the local market.

3.5. Step 5: Specific VA and VASP Assessments

Once the working group has assessed the ML/TF threats, vulnerabilities, and mitigation measures linked to VAs and VASPs at the national level (steps 2–4), jurisdictions must then conduct a more in-depth assessment of the specific VA and VASP services and actors within the jurisdiction (step 5). Detailed guidance on this step is included in sections 5a and 5b. The World Bank’s risk assessment tool requires this exercise because different types of virtual assets and VASPs will face different ML/TF risks and, therefore, by conducting a more in-depth assessment, jurisdictions can increase the effectiveness of their risk-based ML/TF supervision.

5a. Risk Assessment of VA Types

The objective of this exercise is to help authorities build a shared understanding of the ML/TF threats, vulnerabilities, and mitigating measures for specific types of virtual assets. To help with this, the World Bank’s tool (see “Virtual Asset” tab) identifies examples of common virtual assets (such as Bitcoin and Ethereum). For each type, the working group must assess a list of key threat, vulnerability, and mitigation indicators. The number of different types of virtual assets the working group will need to assess will depend on whether the jurisdiction is conducting the basic, intermediate, or advanced version of the tool, with jurisdictions assessing a greater number of more complex VA types for the higher tiers (see table 3.7).

The World Bank’s tool also provides flexibility for jurisdictions to add new types of coins as relevant, bearing in mind that the adoption of specific VAs can evolve quickly for both legitimate and criminal users. Once a jurisdiction has completed this exercise, the tool automatically generates a heatmap showing the relative ML/TF risks associated with each type of virtual asset (see output 7a) to help inform the jurisdiction’s supervisory and law enforcement efforts.

>>>

Table 3.7 Scope of VA Assessment by Tier of Module

Module tier	Virtual asset types to be assessed
Basic module	<ul style="list-style-type: none">○ Bitcoin○ Other (left blank for the working group to edit as relevant)
Intermediate module	<ul style="list-style-type: none">○ Bitcoin○ Privacy coins○ Stablecoins○ Other (left blank for the working group to edit as relevant)
Advanced module	<ul style="list-style-type: none">○ Bitcoin○ Ethereum○ Privacy coins○ Stablecoins○ Non-fungible tokens (when used for investment or payment purposes).○ Other [For this section, jurisdictions completing the advanced tool are encouraged to consider assessing (a) any prominent types of governance tokens when used for investment and payment purposes, (b) platform-issued tokens, (c) wrapped/bridged assets (which represent another asset on a different blockchain), or a combination of these.]

When completing this exercise, jurisdictions will need to gather information from a wide range of public and private sector sources. See table 3.8 for additional data sources specific to each question.

>>>

Table 3.8 Additional Guidance on Completing the VA Assessment

Topic	Variable description	Assessment ratings	Guidance
Threats	<p><i>Prevalence of market share</i></p> <p>What proportion of the virtual asset market in your jurisdiction involves this virtual asset, measured by market cap and transaction volume?</p>	<p>Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown</p>	<p>The objective of this indicator is for the jurisdiction to assess the relative importance of this type of virtual asset for VA activity in the jurisdiction. The working group may want to consider the following:</p> <p>Primary sources</p> <ul style="list-style-type: none"> • Data provided by domestic VASPs, traditional financial institutions, or other private sector representatives on assets held or transaction flows linked to this specific virtual asset type • Data from the tax authorities about the prevalence of this virtual asset in tax and revenue declarations <p>Secondary sources</p> <ul style="list-style-type: none"> • Open-source market reports on the importance of this virtual asset type for the jurisdiction's VA market <p>As there is no definitive and unified source of data on transaction flows by asset, the response to this question will likely need to be based on high-level judgments and estimations rather than on an exact quantitative assessment.</p>

Threats	<p><i>Money laundering</i></p> <p>To what extent is there evidence of criminals using this type of virtual asset to launder funds?</p>	Unknown, not applicable, to a small extent, to a medium extent, to a large extent, to a very large extent	<p>The working group should consult the following sources when reaching an assessment for these variables:</p> <p>Primary sources</p> <ul style="list-style-type: none"> The extent to which certain virtual assets appear in STRs; ML/TF or predicate investigations, prosecutions, or convictions; or in asset recovery cases Intelligence from law enforcement on the (a) extent of access to darknet markets by local consumers and (b) the prevalence of the virtual asset type on the darknet Secondary sources Private sector inputs and perceptions on the extent to which criminals, terrorists, and darknet users may be accessing the virtual asset type Market reports from the FATF and blockchain analytics companies on the ML/TF risks linked to specific VAs <p>If no official data are available, jurisdictions should use secondary sources to estimate.</p>
	<p><i>Terrorist financing</i></p> <p>To what extent is there evidence of terrorists and/or their supporters using this virtual asset to finance their activities?</p>		
	<p><i>Darknet/sanctions exposure</i></p> <p>To what extent is there evidence of this virtual asset being linked to darknet/ransomware activities and/or used to send or receive transactions to and from jurisdictions under international sanctions?</p>		
Vulnerabilities	<p><i>Pseudonymity/traceability</i></p> <p>To which extent do the inherent characteristics of this virtual asset and its blockchain facilitate anonymity (for example, through decentralization or obfuscating tracing)?</p>	Unknown, not applicable, to a small extent, to a medium extent, to a large extent, to a very large extent	<p>When assessing this variable, jurisdictions could consider the following:</p> <ul style="list-style-type: none"> The extent to which this virtual asset type or its blockchain has built in privacy features A high use of this type of virtual asset on decentralized platforms
	<p><i>Peer-to-peer use^a and DeFi</i></p> <p>To which extent is this virtual asset used in P2P transactions outside the formal financial system (for example via social media or informal brokers)?</p> <p>Integration with fiat currency</p> <p>To which extent are exchangers, ATMs, OTC desks commonly used to convert cash into this virtual asset (or vice versa, cashing out)?</p>		<p>To inform this assessment, jurisdictions may wish to consider the following:</p> <ul style="list-style-type: none"> Inputs from domestic and/or foreign VASPs on the extent to which this virtual asset type is being used in P2P transactions Market research or open-source data on the prevalence of this virtual asset in P2P transactions To inform this assessment, jurisdictions may wish to consider the following: Inputs from domestic and/or foreign VASPs on the extent to which this virtual asset type is being converted to/from cash <p>Jurisdictions with a high use of cash in general and a material local presence of exchangers and/or ATMs should consider ratings of medium and above.</p>

Mitigations	To which extent are the primary providers offering services in this virtual asset (such as exchangers, OTC desks, ATMs) regulated and complying with their AML/CFT obligations?	Unknown, not applicable, to a small extent, to a medium extent, to a large extent, to a very large extent	<p>When assessing this indicator, jurisdictions should consider the following:</p> <ul style="list-style-type: none"> Which service providers in the jurisdiction are most actively providing services related to this VAs The extent to which such providers are effectively applying AML/CFT preventative measures <p>In cases in which jurisdictions identify that certain virtual assets are used extensively for P2P transactions or on unregulated platforms, they should assign a lower rating to this variable.</p>
	Does the FIU or law enforcement have access to adequate blockchain surveillance tools (including commercial, open-source, or proprietary tools) used by authorities or reporting entities to monitor transactions in this VA and identify illicit activity?		<p>When answering these questions, jurisdictions may want to consider the following:</p> <ul style="list-style-type: none"> The extent to which there are any successful cases within the jurisdiction of this type of virtual asset being traced, frozen, or confiscated The extent to which inherent features of the virtual asset type (such as built in anonymity or speed of transactions) may hinder tracing, seizing, and confiscation The capacity and knowledge of local authorities to trace, seize, or confiscate this type of virtual asset
	Do authorities have the legal and technical capability to identify, freeze, and confiscate assets of this VA linked to criminal activity?		

Note: DeFi = decentralized finance; OTC = over the counter; P2P = peer to peer.

a. The FATF defines peer-to-peer (P2P) transactions as VA transfers conducted without the use or involvement of a VASP or other obliged entity (such as VA transfers between two unhosted wallets whose users are acting on their own behalf).

5b. Risk Assessment of VASP Types

After assessing the risks posed by different types of virtual assets, the working group should then assess the threats, vulnerabilities, and mitigation measures linked to specific VASP types and services. The objective of this exercise is to help authorities understand which types of VASP services present heightened ML/TF risks, so that they can calibrate their supervisory and law enforcement outreach accordingly.

To help structure this exercise, the World Bank tool identifies the key VASP types by category, in line with the FATF's definition. The number of VASP types the working group will need to assess will depend on the module tier level that the working group has selected, with the intermediate and advanced modules requiring jurisdictions to assess a relatively higher number and complexity of different VASP types (see table 3.9). Once a working group has completed this exercise, the tool automatically generates several heatmaps showing the relative ML/TF risks associated with different VASP types (see outputs 7a–7f in the next chapter). In order to accurately assess the ML/TF threats and vulnerabilities, the working group will need to rely on a wider range of information from supervisors, VASPs, and other industry representatives (see relevant information sources in table 3.10).

Domestic versus foreign VASPs

For several VASP types, the assessment requires an evaluation of the ML/TF risks linked to both domestically registered VASPs and foreign VASPs with a material domestic presence—for example, for centralized exchangers, custodial wallet providers, initial coin offering (ICO) providers, and centralized lending/borrowing services. The World Bank's VA risk assessment tool requires a foreign-domestic breakdown for these centralized VASP services in particular because (a) these services are particularly prominent in many jurisdictions, with jurisdictions seeing a higher presence of foreign services being offered, and (b) jurisdictions are generally able to obtain information about the ML/TF risks of foreign centralized services (unlike on decentralized platforms).²³

When deciding which companies to consider for their risk assessment of “foreign VASP with a material local presence,” jurisdictions should take a consistent approach across all stages of the risk assessment (such as across steps 1–5 as previously described). As mentioned, jurisdictions may wish to focus only on those foreign VASPs that have a material physical presence or local client base in the jurisdiction, or they may use other criteria of their choosing.

Centralized versus decentralized services

For the VASP assessment, the World Bank's VA risk assessment tool requires jurisdictions to assess the ML threats and vulnerabilities linked to both centralized financial services (CeFi) and DeFi services. DeFi covers a wider range of services which facilitate P2P activity, often through exchanges or trades facilitated by smart contracts. Examples include decentralized exchanges (such as Uniswap) and decentralized lending and borrowing platforms (such as Aave).

When determining whether a service is decentralized, both the World Bank's risk assessment tool and the FATF require jurisdictions to take a functional approach by focusing on the level of control or influence over the arrangement. Where there is an individual or entity that exerts influence or control over the service or smart contract, then such an arrangement may actually classify as a centralized service (that is, a VASP) and should be subject to AML/CFT regulation. When initiating the VASP assessment, the working group should meet to discuss which type of arrangements with material links to the jurisdiction would classify as decentralized.

Traditional obliged entities and other VA services (miners and mixers)

In order to accurately assess the ML/TF risks related to virtual assets and VASPs, the World Bank's tool requires jurisdictions to assess the extent to which traditional obliged entities (such as banks) interact with and offer VA services. While the World Bank's tool requires an assessment of the banking sector (for all jurisdictions) and the gambling sector (for jurisdictions conducting the intermediate and advanced module), the tool also provides flexibility for jurisdictions to add further traditional obliged entities for assessment as appropriate.

In addition, for jurisdictions completing the intermediate and advanced version of the module, the World Bank's tool recommends that jurisdictions also assess the ML and TF risks linked to other VA services, such as miners and mixers. While such services are typically not considered VASPs, they do play an important role in the VA ecosystem, and therefore understanding their role helps ensure jurisdictions have a comprehensive understanding of ML/TF risks for the sector.

For example, crypto miners play a key role in validating new transactions on public blockchains and are, in return, often rewarded with new cryptocurrency. Although the vast majority of crypto mining is for legitimate purposes, criminals may misuse mining activity—including by comingling criminal proceeds through mining pools (groups of crypto miners which combine their crypto rewards), or by generating criminal proceeds from crypto mining–related crimes (such as cryptojacking).²⁴ Similarly, VA mixing services (also known as tumblers)—which enhance privacy by comingling and mixing user funds—have been known to be misused by criminals to try to hide the origin of illicit proceeds. For jurisdictions completing the intermediate or advanced version of the tool, additional guidance is provided in table 3.10 on how to assess the key threat, vulnerability, and mitigation indicators for these additional services.

Flexibility and adaptability of the VASP Assessment

For all categories of VASPs, the World Bank's tool leaves flexibility for jurisdictions to add new VASP types and services as needed. This flexibility is important given the fast-evolving nature of the sector. If jurisdictions require more flexibility than that already provided by the tool, they should reach out to the World Bank team to discuss the issue.

>>>

Table 3.9 Scope of VASP Assessment by Tier of Module

VASP category	VASP types to be assessed
Exchange and transfer	<ul style="list-style-type: none"> Centralized exchangers Decentralized exchangers Other ATMs Over-the-counter (OTC) exchangers VA payment providers
VA wallets	<ul style="list-style-type: none"> Custodial ("hosted") wallets Noncustodial ("unhosted") wallets
VA investment	<ul style="list-style-type: none"> Issuers of initial coin offerings Stablecoin issuers/providers Other Centralized lending/borrowing services Decentralized lending/borrowing services
Other services	<ul style="list-style-type: none"> VA mixers Other VA miners
Regulated entities (non-VASP)	<ul style="list-style-type: none"> Banks Other Casinos and gambling sites

Key: All tiers = black, intermediate and advanced only = red, advanced only = blue.

Table. 3.10 Additional Guidance on Completing the VASP Assessment

Relevant tabs	Questions	Assessment ratings	Guidance/relevant information sources
1. Exchange and transfer	Threats		
2. VA wallets	<i>Volume and activity</i>	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>When answering this question, jurisdictions can gather data on the size and materiality of activity from the following sources:</p> <p>For domestic VASPs</p> <ul style="list-style-type: none"> Supervisory data on the volume of registered/licensed domestic providers and their turnover (for centralized exchanges) (primary source) Open-source data on the trading volume or scale of service/offering (provided by websites such as CoinMarketCap) Other expert/industry estimates <p>For foreign VASPs</p> <ul style="list-style-type: none"> Information from foreign supervisors on the turnover/size of foreign providers that may be operating within the jurisdiction (primary source) Information from foreign VASPs (primary source) Other industry reports or other open sources <p>When deciding whether a particular service is material/significant, the working group may want to consider its relative importance (compared to either the overall VA sector in the jurisdiction, the overall financial sector in the jurisdiction, or both)</p> <p>While decentralized services may be harder to quantify, the working group may consult blockchain analytics companies, estimates via web traffic, protocol volume, or wallet interactions involving DeFi platforms</p>
3. VA investment	What is the size and volume of the activity/service?		

1. Exchange and transfer 2. VA wallets 3. VA investment	Vulnerabilities		
	<i>Anonymity features</i> Do providers offer services that facilitate anonymity?	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>Examples of services that facilitate anonymity include services involving privacy coins; services which facilitate P2P transactions and/or complex trades (that is, trades on higher-risk blockchains such as TRON); and VA activities that integrate mixing/tumbling services.</p> <p>For jurisdictions completing the intermediate and advanced modules and assessing investment services, the working group should consider the token issuance processes, a lack of transparency in ICO white papers and securities or other filings, use of intermediaries, and potential misuse of decentralized investment vehicles.</p> <p>Notably, decentralized providers will inherently offer higher levels of anonymity, especially if unlicensed for AML/CFT purposes.</p> <p>Information sources may include VASP websites, regulatory filings, STRs, or technical audits.</p>
	<i>High-risk customers</i> Do high-risk customers access this service?		<p>For this indicator, high-risk customers may include politically exposed persons; foreign clients from high-risk jurisdictions for ML, TF, or sanctions evasion; or front companies.</p> <p>The working group may gather information on the nature of exchange/transfer clients from the following:</p> <ul style="list-style-type: none"> • From VASPs directly (for locally registered companies) • From foreign supervisors for foreign VASPs <p>Secondary sources</p> <ul style="list-style-type: none"> • Expert opinions from the public or private sector on the nature of clients • Open-source research and/or blockchain analytics data <p>VASP types with limited customer controls (such as unlicensed exchange types or decentralized platforms) will likely have higher exposure to high-risk clients.</p>
	<i>High-risk coin types</i> Are providers used to buy or sell higher-risk virtual assets?		<p>High-risk coin types include privacy coins (Monero, Zcash) or coins which run on many different blockchains (including higher-risk blockchains such as TRON).</p> <p>Information for this indicator may come from VASPs (via their website or supervisory engagement), blockchain analytics companies, or industry reports.</p> <p>For jurisdictions completing the advanced/intermediate modules, for ICOs working groups may obtain information for this indicator from project white papers or post-ICO trading activity.</p>

<ol style="list-style-type: none"> 1. Exchange and transfer 2. VA wallets 3. VA investment 	<p><i>Use of cash</i></p> <p>Are providers facilitating trade to/from fiat currency (cash) into virtual assets?</p>	<p>Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown</p>	<p>[Note to working groups: This indicator is included only for exchange and transfer and VA investments, but not VA wallets.]</p> <p>The working group should evaluate whether providers or platforms support fiat on/off ramps, especially those involving cash. Sources may include public disclosures, platform terms of service, or STRs involving cash-for-crypto trades. VA companies that have weak AML/CFT controls may facilitate higher use of cash.</p> <p>In-person OTC providers (such as ATMs) are inherently likely to facilitate activity in cash. Similarly, jurisdictions that have both a high use of cash generally and a material VASP sector should consider rating this indicator more highly.</p>
<p>Mitigation measures Note: In this section, the answer “high” indicates a high level of mitigation.</p>			
	<p><i>CDD</i></p> <p>Are providers effectively implementing preventive measures, including customer onboarding and due diligence (KYC/CDD)</p>	<p>Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown</p>	<p>For this question, jurisdictions should consider the following:</p> <ul style="list-style-type: none"> • The extent to which providers are subject to AML/CFT preventive measures, particularly customer due diligence and onboarding requirements • The extent to which providers are complying with such requirements in practice (that is, the effectiveness level) <p>For domestic VASPs, jurisdictions may consult</p> <ul style="list-style-type: none"> • Findings from supervisory engagement to domestic VASPs • Information provided by local VASPs • Open-source research (via VASP websites, and so on) <p>For foreign VASPs with a material local presence, jurisdictions may consult</p> <ul style="list-style-type: none"> • Information provided by home supervisors or via foreign VASP websites • Any relevant findings from the home supervisor’s latest FATF assessments (FATF’s Recommendation 15, or Immediate Outcomes 3 or 4) • Open-source information on AML/CFT requirements in the jurisdiction of establishment (if known)

<ol style="list-style-type: none"> 1. Exchange and transfer 2. VA wallets 3. VA investment 	<p><i>Transaction monitoring</i></p> <p>Do providers effectively monitor and file suspicious transaction reports (STRs) and apply the FATF's Travel Rule?</p>	<p>Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown</p>	<p>In addition to the sources previously mentioned, jurisdictions may wish to consider the following:</p> <p>For domestic VASPs, jurisdictions may consult</p> <ul style="list-style-type: none"> • Domestic requirements and any supervisory findings on Travel Rule implementation • Any data from the FIU on STR reporting. Low STR volume despite high activity may point to weak monitoring. <p>For foreign VASPs, jurisdictions may consult</p> <ul style="list-style-type: none"> • Data from a foreign FIU or supervisor on STR reporting by foreign VASPs • Information from FATF reports on Travel Rule compliance • Whether or not providers are regulated (in the case of unregulated or decentralized providers, the rating for this indicator will need to be lower)
	<p><i>Supervision and monitoring</i></p> <p>Are supervisors effectively supervising and monitoring AML/CFT requirements?</p>		<p>In addition to the sources mentioned, jurisdictions may wish to consider the following:</p> <p>For domestic VASPs, jurisdictions may consult</p> <ul style="list-style-type: none"> • The capacity of local supervisors to monitor and enforce AML/CFT requirements. For example, jurisdictions should consider whether supervisors are conducting regular inspections of registered providers in practice and can identify discrepancies between VASPs' chain presence and their reported activity. • Any findings in FATF reports on the effectiveness of supervision <p>For foreign VASPs, jurisdictions may consult</p> <ul style="list-style-type: none"> • Information from FATF reports on VA supervision in the home jurisdiction (if known) • Open-source information on supervision of foreign VASPs in their home jurisdiction (if known) • If not possible to obtain any information, jurisdictions should assign a rating of "unknown". <p>Jurisdictions should consider whether or not providers are regulated (in the case of unregulated or decentralized providers, the rating for this indicator will need to be lower). For unregulated or decentralized services, the working group should assign a low or very low rating for this indicator.</p>

<ol style="list-style-type: none"> 1. Exchange and transfer 2. VA wallets 3. VA investment 	<p><i>Law enforcement</i></p> <p>Is law enforcement able to obtain information from providers for ML/TF investigations?</p>		<p>In addition to the sources mentioned, jurisdictions may wish to consider the following:</p> <p>For both domestic and foreign VASPs</p> <ul style="list-style-type: none"> • The legal authority and practical ability of local law enforcement, intelligence agencies, and supervisory enforcement teams (as applicable) to request and obtain data from VASPs • Whether there have been any cases in practice of law enforcement being able to obtain information from domestic or foreign VASPs, and the response times and quality of data received in such cases • Legal gateways for information sharing <p>For foreign VASPs</p> <ul style="list-style-type: none"> • Consider the extent to which local law enforcement can obtain information from foreign counterparts on foreign VASPs
<p>Other services (mixers, miners)</p>	<p>Threats</p>		
	<p><i>Volume and activity</i></p> <p>To what extent does the local population access or participate in this service? What volume of assets passing through the service has links to local users or local wallets?</p>	<p>Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown</p>	<p>The working group should estimate access to these services using blockchain analytics, public reports, or anecdotal indicators (including social media and online forums). For mixers, assess the extent to which local wallets have transacted with known mixing services. For miners, estimate local mining participation through statistics such as node geolocation or mining pool membership statistics.</p>
	<p><i>Illicit financial flows</i></p> <p>To what extent has the service been used in any known ML, ransomware, darknet market, or terrorism financing cases?</p>		<p>The working group should review typologies, STRs, and law enforcement cases that implicate these services in illicit finance. For example, mixers have been repeatedly linked to laundering ransomware proceeds and darknet market funds, thus they represent a high risk. Mining operations may be misused to obfuscate the origin of illicit funds or to cash out criminal profits without triggering STRs.</p>

Other services (mixers, miners)	Vulnerabilities		
	<p><i>Anonymity features</i></p> <p>To what extent does the service serve the purpose of anonymizing transactions?</p>	<p>Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown</p>	<p>The working group should assess the degree to which these services prevent traceability of funds. Mixers (centralized or protocol based) are specifically designed to break transaction trails by pooling and redistributing funds. Mining pools may anonymize fund origins if rewards are distributed without KYC (or if they act as conduits for mixing-like activity).</p> <p>Mixers: This may include the availability of centrally administered mixing services and decentralized, protocol-based mixing services. Miners: This may include mining pools with inadequate KYC controls or any other means by which mining rewards are distributed in an anonymized fashion.</p>
	<p><i>Interoperability</i></p> <p>Is there evidence of interoperability between the service and other domestic VASPs or foreign VASPs with material domestic presence?</p>		<p>The working group should use blockchain analytics or supervisory insights to identify connections between these services and regulated or unregulated VASPs. Mixers often receive funds from exchangers and return them to different exchangers or wallet providers, complicating tracing.</p>
	<p><i>High-risk customers</i></p> <p>Is there evidence of high-risk customers (such as PEPs) accessing this investment type?</p>		<p>The working group should identify whether PEPs or sanctioned persons use these services by reviewing blockchain forensics, STRs, or law enforcement investigations.</p>

Other services (mixers, miners)	<i>Cashing-out</i> Is there evidence of mining rewards (from domestic mining activity) sold via unregulated exchanges or other unregulated P2P platforms?		The working group should identify whether PEPs or sanctioned persons use these services by reviewing blockchain forensics, STRs, or law enforcement investigations.
	Mitigations		
	<i>Customer onboarding and due diligence</i> Are providers of this service effectively implementing preventive measures, including customer onboarding and due diligence (KYC/CDD)?	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	The working group should assess whether providers verify users and implement risk-based due diligence. Mixers, especially decentralized ones, typically do not conduct any onboarding.
	<i>STR monitoring</i> Do regulated VASPs effectively monitor and file suspicious transaction reports (STRs), and apply the FATF's Travel Rule?		Evaluate whether VASPs can detect and report transactions linked to these services. Mixers may be detected through transaction patterns or known wallet associations, but not all VASPs are equipped to identify them.

Other services (mixers, miners)	<i>ML/TF awareness</i> Have supervisors or the FIU done public outreach on AML/CFT issues, including risks related to these entities or providers of these services?		The working group should determine whether awareness campaigns, advisories, or guidance have addressed risks associated with anonymizing services.
	<i>Supervision and monitoring</i> Are supervisors effectively supervising and monitoring AML/CFT requirements? For mixers, have restrictions been imposed or public awareness efforts mitigated risks?	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	The working group should assess how and whether supervision is conducted. For certain entities, this may not be possible. For example, centralized mixers are generally not supervised because they exist to obfuscate transaction flows and funds provenance, but restrictions on their use may apply through law enforcement or sanctions regimes.
	<i>Law enforcement</i> Are blockchain analytics tools used by the FIU? Can law enforcement detect use of this service and take enforcement actions, as necessary?		Determine whether investigative agencies, intelligence agencies, and supervisory enforcement teams (as applicable) use tools to identify illicit behavior involving these services. For mixers, blockchain analytics can sometimes identify usage patterns even when transaction trails are broken. Mining-related transactions may require contextual data (such as Internet Protocol (IP) or pool addresses) to identify nodes that support attribution or enforcement.

Regulated entities (non-VASPs)	Threats		
	<i>Volume and activity</i> Extent to which the regulated entity type has clients who are VASPs and/or individuals buying or selling virtual assets or engaging in VA activity.	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>The working group should assess the degree of exposure regulated entities have to VASP clients or individuals conducting VA-related transactions. This can be informed by supervisory reporting, STRs, or data from correspondent banking and payment platforms.</p> <p>For example, banks may provide accounts or fiat on/off ramps to VASPs and VA users. Casinos and online gambling platforms may accept VA payment or gambling.</p>
	<i>Illicit financial flows</i> Evidence of the regulated entity type in the jurisdiction being misused for ML or TF cases involving virtual assets (based on STRs filed by the regulated entity type)		<p>The working group should review STR data and case studies involving misuse of these sectors in the context of VA-related laundering or financing.</p> <p>For example, banks have been used to layer or integrate illicit VA proceeds, particularly where the origin of funds is obscured before deposit. Casinos and gambling sites, particularly online VA gambling platforms, may be misused to convert VA into virtual chips or prizes that are then cashed out to fiat funds.</p>
	Vulnerabilities		
	<i>Decentralization</i> Extent to which the local population are using decentralized versions of the regulated entity type (such as smart contract–based sites, no clear administrator)	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	<p>The working group should assess the use of decentralized alternatives such as DeFi lending platforms or blockchain-based gambling sites. This may be based on user traffic, social media activity, or blockchain analytics. For casinos and gambling services, decentralized betting protocols or blockchain casinos with no KYC requirements present high anonymity and accessibility.</p>

Regulated entities (non-VASPs)	High-risk customers Evidence of high-risk customers accessing the regulated entity type (such as PEPs, vulnerable groups, or foreign actors)	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	The working group should determine whether high-risk clients, such as PEPs or foreign nationals, are known to access services provided by these entities. Sources include customer risk profiles, STRs, or supervisory reviews. Banks may serve PEPs, offshore companies, or VA traders with opaque financial profiles. Casinos and gambling services can attract high-risk users because of their weak controls and cross-jurisdictional nature.
	High-risk coin types Extent to which the entity type is providing services (such as payments) in high-risk coin types.		Assess whether banks or casinos directly or indirectly handle VAs or deal with clients holding VAs with anonymity-enhancing features (such as privacy coins or stablecoins, given their significant misuse in ML cases). Sources may include transaction monitoring data, payment processor disclosures, or STRs. Banks may inadvertently facilitate withdrawals linked to such coins via third-party exchangers. Casinos may accept VA payments directly or via intermediaries and may not distinguish between standard and high-risk coin types.
	Mitigations		
	VA knowledge Strength of the awareness of ML/TF risks involving virtual assets within the regulated entities' sector	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	The working group should assess the level of awareness within the sector of VA-related risks. This may include training programs, public guidance, or self-assessments. Banks with stronger awareness typically implement VA-specific transaction screening and customer risk scoring.
	Customer onboarding and due diligence Strength of the sector's onboarding and ongoing due diligence for customers that are VASPs or individuals conducting VA activities		Evaluate whether regulated entities apply enhanced onboarding procedures and risk-based due diligence for clients engaged in VA activities.

Regulated entities (non-VASPs)	<i>Transaction monitoring</i> Ability of the regulated entities to effectively monitor and file suspicious transaction reports involving VAs and apply the FATF's Travel Rule	Very high, high, medium-high, medium, medium-low, low, very low, not applicable, unknown	Assess how effectively the sector can identify and report suspicious VA-related activity. Sources may include STR quality reviews and case studies. Banks often rely on blockchain analytics tools and red flags to identify unusual VA activity, but effectiveness varies. Casinos may not have monitoring tools for VA deposits or winnings conversion, limiting detection unless the subject is cashing out through fiat interfaces.
	<i>Supervision and monitoring</i> Extent to which supervisors are conducting outreach to the sector on AML/CFT issues related to virtual asset activities and practices		Determine if authorities have issued guidance, hosted workshops, or provided training specific to VA risks for non-VASP sectors. For banks and casinos and gambling services, supervisors may provide tailored guidance or require enhanced reporting.
	<i>Law enforcement</i> Extent to which law enforcement can obtain information on financial flows linked to virtual assets from regulated entities for ML/TF investigations		Evaluate practical access to data from banks and casinos in support of investigations. Banks typically maintain customer and transaction data that can assist in tracing VA-related flows. Casinos, especially online platforms or those in offshore jurisdictions, may present challenges to data access, particularly if VAs are accepted outside of formal reporting channels.

Note:CDD = customer due diligence.



4. Tool Outputs

Using the input provided and built-in formulas, the World Bank’s VA risk assessment tool generates visual outputs that authorities may use to inform their activities and action plan following the risk assessment. This chapter provides additional information for the working group on how to interpret and use the outputs.

4.1. Output 1: Risk Overview

The first output, shown in the “Output 1—Risk Overview” tab provides a comprehensive overview of the key risk scores computed by the tool based on the jurisdiction’s input. Figure 4.1 explains how to read the Risk Overview.



Figure 4.1. Subcomponents of Risk Overview

Example	Guidance												
<table><tr><td>Money Laundering Threat</td><td>Medium</td></tr><tr><td>Internal/Incoming incidence of use of Virtual Assets</td><td>Medium-High</td></tr><tr><td>External/Outgoing incidence of use of Virtual Assets</td><td>Very Low</td></tr><tr><td>Terrorist Financing Threat</td><td>Low</td></tr><tr><td>Internal/Incoming incidence of use of Virtual Assets</td><td>Low</td></tr><tr><td>External/Outgoing incidence of use of Virtual Assets</td><td>Low</td></tr></table>	Money Laundering Threat	Medium	Internal/Incoming incidence of use of Virtual Assets	Medium-High	External/Outgoing incidence of use of Virtual Assets	Very Low	Terrorist Financing Threat	Low	Internal/Incoming incidence of use of Virtual Assets	Low	External/Outgoing incidence of use of Virtual Assets	Low	<p>This part of the Risk Overview summarizes the ML/TF threat ratings faced by the jurisdiction. This score is automatically calculated based on the inputs in the “National ML and TF Techniques” tab. The results are broken down for ML and TF separately to help authorities understand their exposure.</p> <p>In the example results provided on the left, the outcome indicates that the jurisdiction faces higher ML threats than TF threats and that generally the threats are either incoming or internal, suggesting that the jurisdiction may be a destination for ML involving VAs.</p>
Money Laundering Threat	Medium												
Internal/Incoming incidence of use of Virtual Assets	Medium-High												
External/Outgoing incidence of use of Virtual Assets	Very Low												
Terrorist Financing Threat	Low												
Internal/Incoming incidence of use of Virtual Assets	Low												
External/Outgoing incidence of use of Virtual Assets	Low												

National Vulnerability (overall score)	Medium-Low
General National Inherent Vulnerabilities	Medium-High
Inherent Vulnerability - Local	Low
Size and Value of Sector	Low
Activity Delivery	Low
Client Base	Medium-Low
Services Delivered	Very Low
Cash & Virtual Assets	Medium-Low
Inherent Vulnerability - Foreign	Medium
Size and Value of Sector	Medium
Data Quality	Medium
Activity Delivery	Medium-High

This part of the Risk Overview shows the national vulnerabilities scores. The ratings for this are automatically generated on the basis of the jurisdiction's inputs for the "National Inherent Vulnerability" tab. Inherent vulnerability is the vulnerability without accounting for any mitigation measures.

In the example provided on the left, the hypothetical results show that for this jurisdiction, foreign VASPs represent a greater vulnerability (with a medium vulnerability) than domestic VASPs (which represent a low vulnerability).

Inherent Risk - ML	Medium
Inherent Risk - TF	Medium-Low

The inherent risk levels of ML and TF are based on the combination of threats and inherent vulnerabilities. *Inherent risk* is the overall risk level before mitigation measures have been considered.

Mitigation Measures	High
<i>Technical Compliance:</i>	
Risk Assessment & Risk Management	Very High
Licensing/Registration & Supervision	High
AML/CFT Preventative Measures	High
International Cooperation	Very High
<i>Effectiveness of Controls:</i>	
Implementation of AML/CFT preventative measures (local VASPs)	High
Implementation of AML/CFT preventative measures (offshore VASPs)	Medium-Low
Other	High

This part of the output displays the strength of mitigation measures. This is automatically generated on the basis of the jurisdiction's inputs for the "National Mitigation Measures" tab. The output breaks down the technical compliance and the effectiveness separately.

In the example results provided on the left, the jurisdiction's own AML/CFT controls are assessed to be very effective, whereas the mitigations measures taken by foreign VASPs are deemed less effective.

Residual Risk - ML	Low
Residual Risk - TF	Low

The overall residual risk scores for ML and TF build on all previous scores, adjusting the inherent risk score (a combination of threat and vulnerability) in light of applicable mitigation measures.

In this example on the left, both ML residual risk and TF residual risk are low because of effective mitigation measures. For jurisdictions with weaker AML/CFT controls, the mitigation measures will have less impact reducing the overall risk.

4.2. Output 2: ML Cases

Output 2 displays several charts based on the statistics that the jurisdiction gathers on ML cases and intelligence involving VAs (see data inventory in “General Mapping” tab). See additional details in figure 4.2.



Figure 4.2. Charts Generated by Output 2—“ML Cases”



4.3. Output 3: Techniques

Output 3 generates a prioritization of the ML/TF techniques assessed in the ‘ML/TF Techniques’ tab to assist jurisdictions in their supervisory and enforcement outreach. Specifically, the output automatically identifies the top 15 ML/TF techniques in order of importance, based on the jurisdiction’s assessment of the known and suspected prevalence of each technique. For techniques identified as “high” or “very high”, jurisdictions should consider taking immediate attention, including pursuing targeted outreach to the private sector to help raise awareness for related red flags. See the example in figure 4.3.

>>>

Figure 4.3. Example of Prioritization Table for MLTF Techniques

National Highest Risk Techniques -		
No.	Description	Rating
2	Use of mixer or tumbler services to hide the origin and recipient of transactions (whether centralised mixing services or decentralised services such as Coinjoin)	Very High
3	Use of VAs with enhanced privacy features (e.g. Monero).	Medium
1	Chain Hopping - Rapidly swapping VAs between blockchains.	Medium
5	Use of privacy wallets with built-in mixing features	Medium-Low
4	Use of peer-to-peer platforms facilitating direct VA trades between users without AML/CFT controls	Very Low

Understanding the most prevalent ML/TF techniques allows policymakers, supervisors, law enforcement, and other national authorities to do the following:

- **Recognize suspicious behavior.** Techniques illustrate specific red flags and transaction patterns that can alert stakeholders to the presence of illicit activity.

- **Improve risk assessments.** Jurisdictions can tailor national and sectoral risk assessments by mapping domestic VASP activity against known techniques.
- **Strengthen mitigation strategies.** By understanding how VASP abuse occurs in practice, jurisdictions can adapt supervisory frameworks, AML/CFT controls, and investigative capabilities to respond more effectively.
- **Enhance public-private and cross-border dialogue.** Techniques create a common language between the public and private sectors, which can be used in STRs and any threshold-based filings required by the national AML/CFT legislation in place.

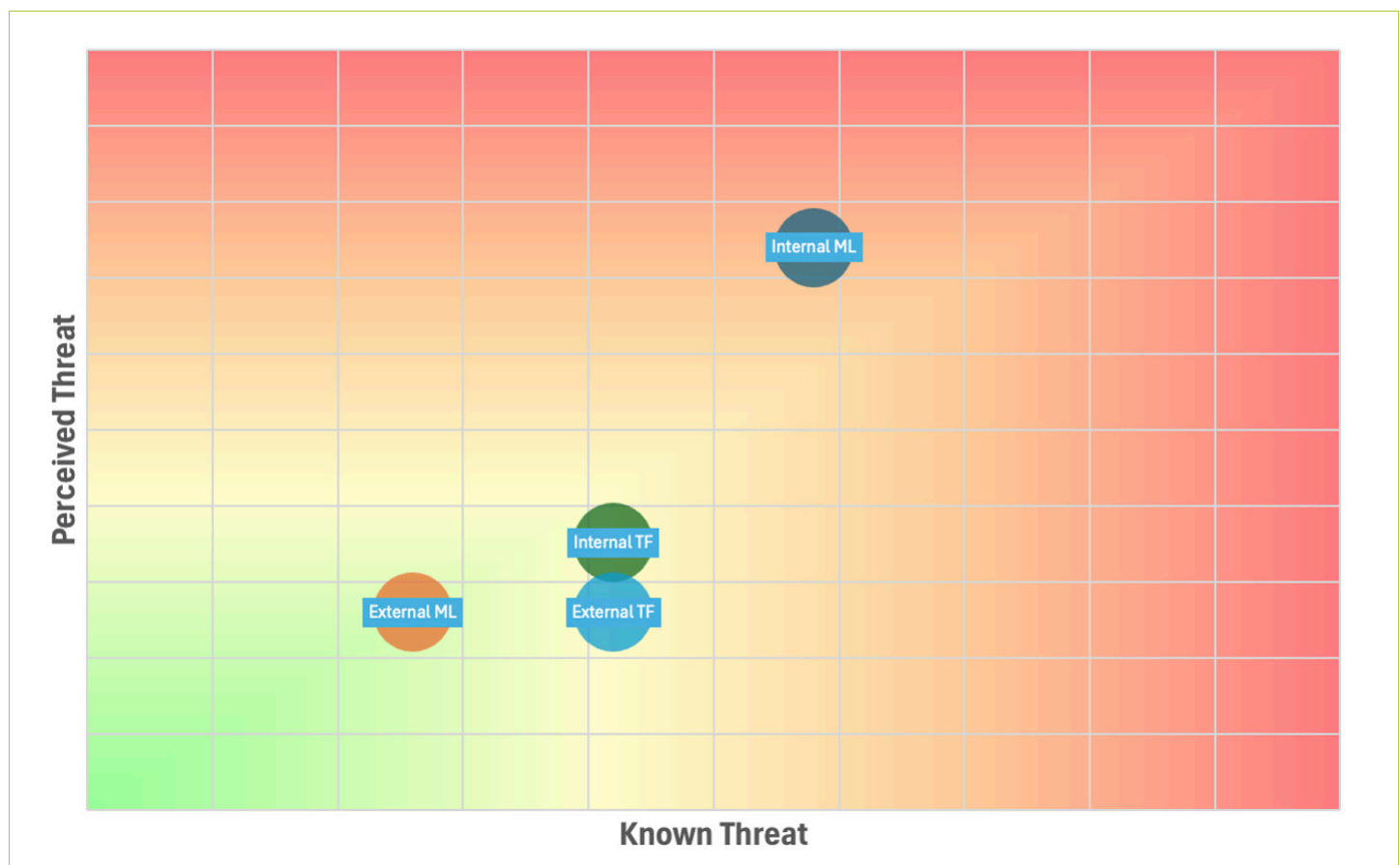
4.4. Output 4: Criminal Use of VAs

This output allows the working group to identify the relative levels of internal/incoming and outgoing ML and TF threats (see example in figure 4.4). The “Internal/incoming ML” threat refers to the threat arising from domestic predicate offenses or foreign overseas predicate offenses in which the proceeds are laundered domestically through VA and VASP activities in the jurisdiction. Similarly, the “Internal/Incoming TF” threat refers to the threat of funds being used to support terrorists and their activities within the jurisdiction.

In contrast, the “Outgoing ML or TF” threat refers to the threat of criminal proceeds or other funds being moved out of the jurisdiction to be laundered or finance terrorism abroad. The example provided in figure 4.4 shows that the jurisdiction has a high internal ML threat and a relatively lower external threat. This suggests that there is significant threat facing local companies that offer VA services, requiring strong AML/CFT controls and supervisory outreach to the sector.

>>>

Figure 4.4. Overview of Internal/Incoming versus Outgoing ML and TF Threat Levels



4.5. Output 5: Technical Compliance

This output summarizes a jurisdiction’s level of technical compliance with FATF Recommendation 15 (see example in figure 4.5) and may inform the prioritization of any legislative or regulatory reforms that may be required. The results for this chart are based on the self-assessment inputs that the working group provides in the “National Mitigation Measures” tab. For areas where technical compliance is weak, the graph line will appear closer to the center of the spider chart indicating a deficiency (as marked in red). For example, in figure 4.5 the result shows that the licensing/registration regime represents the main gap in the jurisdiction’s regulatory framework for VASPs.

>>>

Figure 4.5. Overview of Technical Compliance

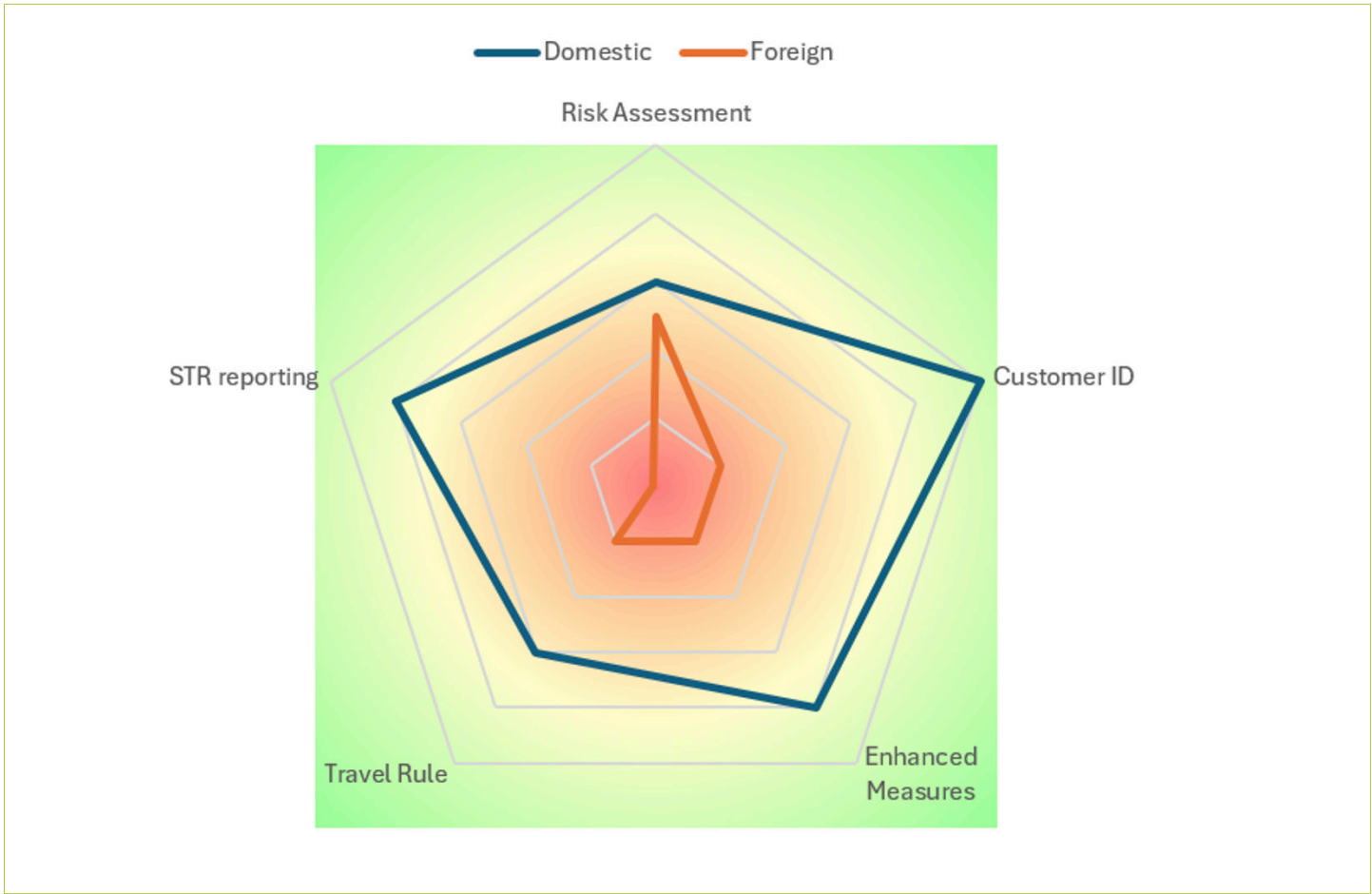


4.6. Output 6: Preventive Measures for VASPs

Output 6 compares the effective implementation of AML/CFT preventive measures by domestic versus foreign VASPs with a material local presence. This chart is based on the jurisdiction’s inputs for the “National Mitigation Measures” tab. Similar to the previous output, the closer the graph line is to the center of the spider chart (that is, the red part of the graph), the larger the deficiencies. For example, in figure 4.6, the effectiveness of domestic VASPs in implementing AML/CFT preventive measures is consistently considered stronger than for foreign VASPs with a material local presence. This finding suggests that additional supervisory engagement may be required to oversee foreign VASPs operating in the jurisdiction.

>>>

Figure 4.6. Summary of Effectiveness of Preventive Measures Taken by Local and Foreign VASPs



4.7. Outputs 7a to 7f: Specific VA and VASP Types

Outputs 7a to 7f provide a visualization of the relative importance of different VA and VASP types, based on the jurisdiction’s inputs for the VA and VASP assessments (see step 5 in section 3.5). Specifically, the graphs map the various VAs and VASP types by the level of threat and vulnerability (which are adjusted for mitigation measures). The resulting graphs therefore provide a helpful visualization for jurisdictions of the overall residual risk presented by different VA and VASP types.

Ideally, jurisdictions should use these results to inform their risk-based supervision and enforcement actions. For example, in the hypothetical example provided in figure 4.7, the results show that privacy coins and stablecoins represent the highest ML/TF risk for the jurisdiction, whereas Bitcoin presents a relatively lower risk. In such a situation, the jurisdiction may therefore need to conduct enhanced training for authorities and provide supervisory outreach on privacy and stable coins. For VASP types, outputs 7b to 7f provide an overview of the risk level by different VASP categories (such as exchange and transfer, custodial services, investment, and other services).²⁵ In the example provided in figure 4.8, the results show that decentralized exchangers and local ATMs present the most material ML/TF risks, suggesting additional outreach to these entity types is needed.

>>>

Figure 4.7. Overview of Threats and Vulnerabilities by Type of Virtual Asset

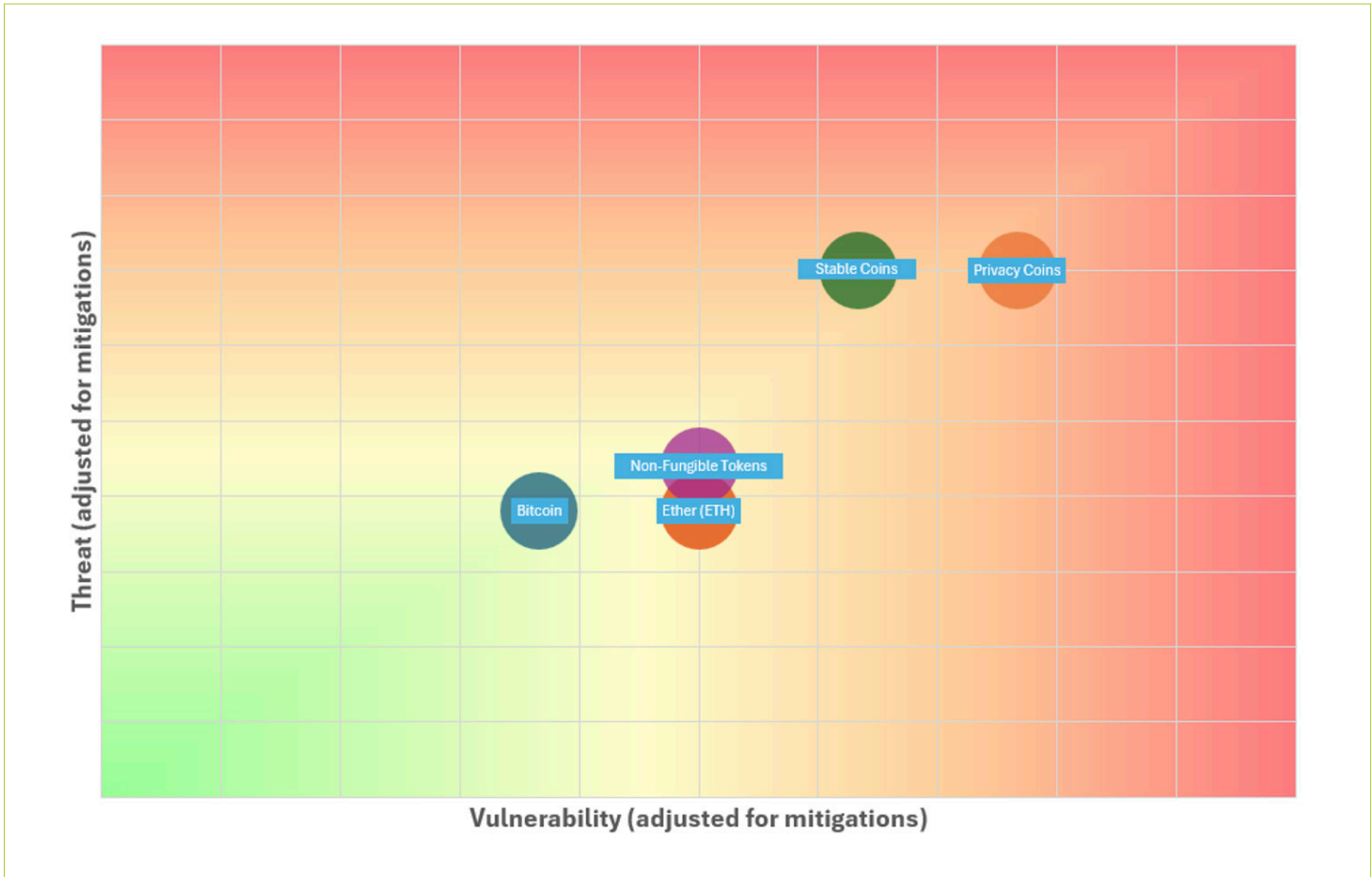
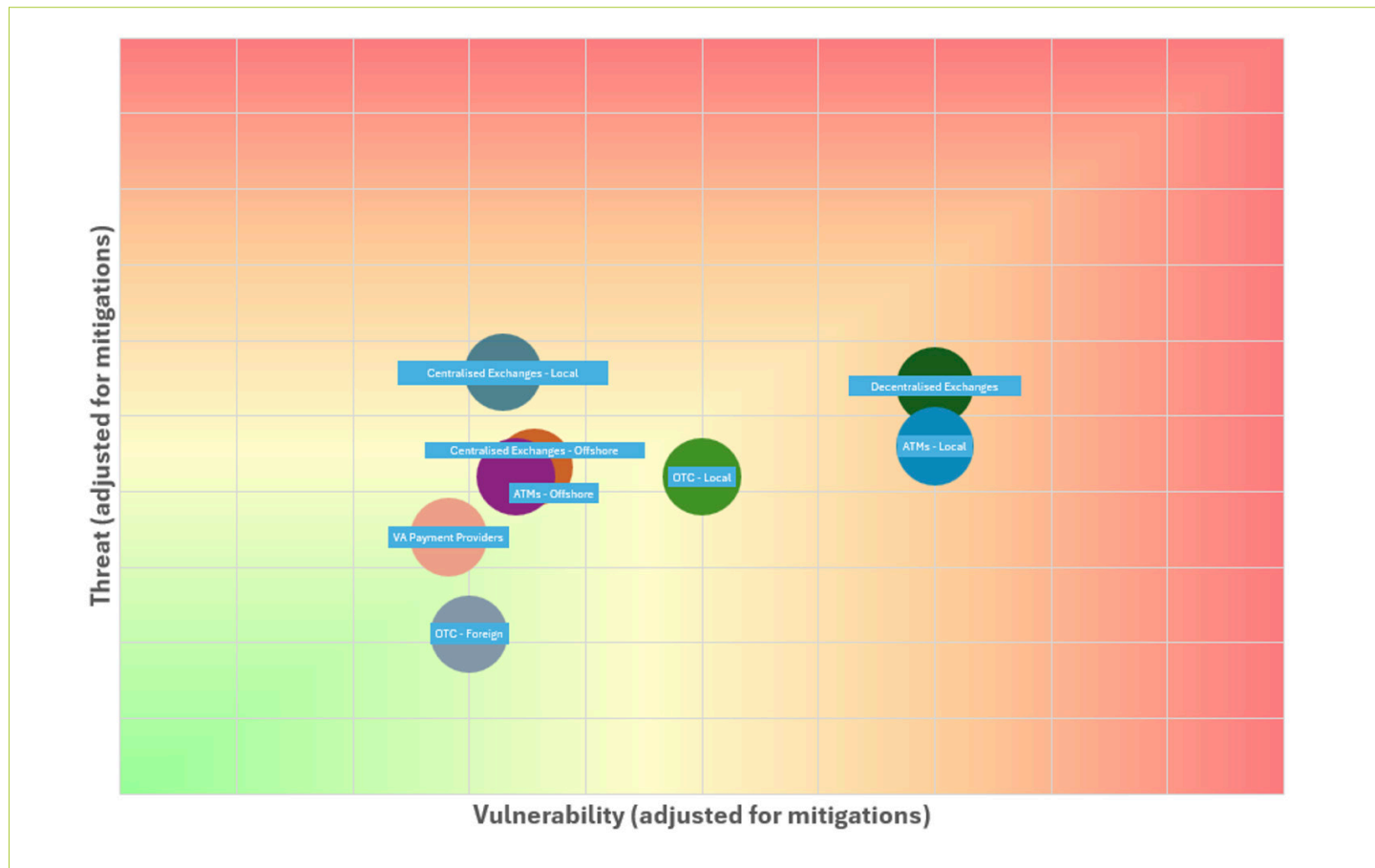


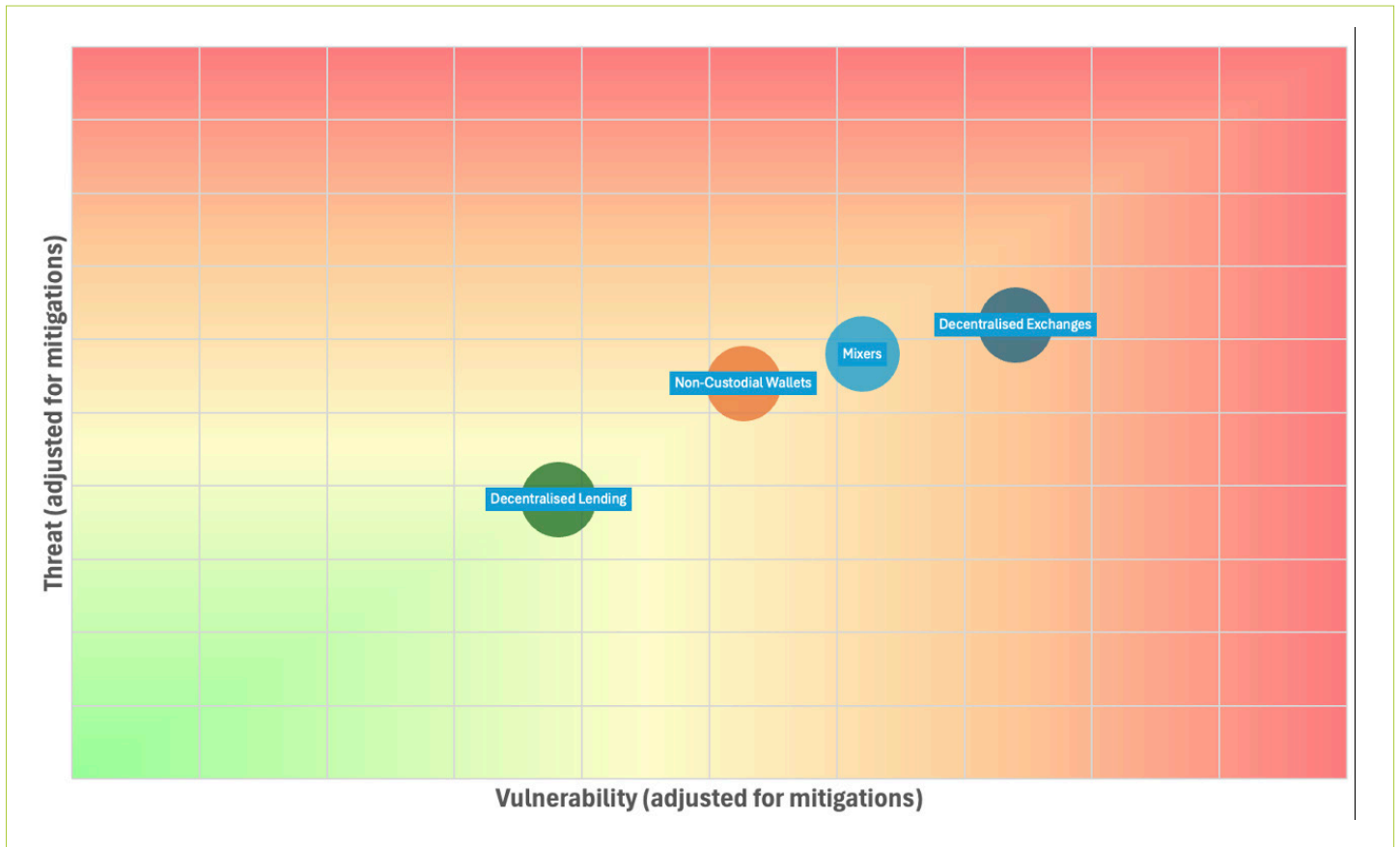
Figure 4.8. Overview of Threats and Vulnerabilities Related to Different Types of Exchangers



4.8. Outputs 8a and 8b: DeFi and CeFi

The final two output charts present the ML/TF risks related to centralized and decentralized VA services,²⁶ respectively. The objective of this output is to help jurisdictions understand the relative ML/TF risks across different VASP categories. For example, in figure 4.9, the output shows that across the different decentralized services and activities, the ML/TF risks are highest for decentralized exchangers. In this scenario the jurisdiction should consider doing enhanced and targeted outreach to (a) raise awareness about the potential ML/TF risks related to such platforms and (b) review whether such platforms are, in fact, decentralized in practice or whether there is an individual or company behind such platforms that may warrant AML/CFT regulation.

Figure 4.9. Overview of ML/TF Risk Profiles of Decentralized Finance Services





5. Glossary



Centralized Exchanger	A virtual asset centralized exchanger (CEX) is a platform, managed and operated by a central entity, through which users can trade digital assets (like cryptocurrencies) with each other. These exchangers act as intermediaries, holding users' assets and facilitating transactions.
Custodial Hot Wallet	A custodial hot wallet is a cryptocurrency wallet in which a third party, like a centralized exchange, holds and manages the private keys for the user, while also being an online or internet-connected wallet (hot). This means users do not have direct control over their private keys and thus rely on the custodian for security and transactions. For comparison, see also Noncustodial Wallets, through which users retain full control of their keys and store them offline for enhanced security.
Decentralized Exchange	A decentralized exchanger (DEX) is a peer-to-peer marketplace in which cryptocurrency traders can exchange assets directly without the involvement of a central authority like a traditional exchange. Instead of a centralized intermediary, DEXs utilize smart contracts on a blockchain to facilitate transactions.
Decentralized Finance (DeFi)	Decentralized finance (DeFi) refers to financial services provided through arrangements that use smart contracts on distributed ledgers (blockchain technology), enabling peer-to-peer transactions without relying on traditional financial intermediaries.
DeFi Lending	DeFi lending is a decentralized financial service through which users can lend or borrow cryptocurrencies directly from each other, bypassing traditional financial intermediaries like banks. It operates using smart contracts on blockchain networks, allowing for transparent and trustless lending and borrowing activities.
Distributed Ledger Technology (DLT)	DLT refers to a type of technology protocol that enables simultaneous access, validation, and updating of an immutable ledger (digital record) distributed across multiple computers (and typically, across multiple entities or locations)—that is, DLT creates a distributed digital database.
FATF Travel Rule	Under Financial Action Task Force (FATF) Recommendation 16, the Travel Rule requires virtual asset service providers (VASPs) and other entities involved in virtual asset (VA) activities to obtain, hold, and transmit specific originator and beneficiary information immediately and securely when conducting VA transfers.
Fiat-to-Fiat Exchange	This is an exchange between one or more forms of virtual assets for or on behalf of another natural or legal person.
Inherent Risk	Inherent risk is the level of money laundering (ML) and terrorist financing (TF) risk before applying any controls or mitigation measures. It is based on the combination of threats and vulnerabilities and reflects the exposure to risk in the absence of any mitigating actions.

Initial Coin Offering (ICO)	An initial coin offering is the cryptocurrency industry's equivalent of an initial public offering. A company seeking to raise money to create a new blockchain app or service with a cryptocurrency can launch an ICO as a way to raise funds.
Initial Coin Offering Provider	An ICO provider is any natural or legal person who is not covered elsewhere under national legislation, and as a business, participates in or provides financial services related to an issuer's offer and/or sale of a virtual asset for or on behalf of another natural or legal person.
Known Threat	This refers to the level of ML/TF threat that is supported by concrete evidence such as investigations, prosecutions, convictions, supervisory findings, or financial intelligence unit (FIU) disseminations. It reflects actual, documented instances or patterns of criminal activity.
Peer-to-peer (P2P) Transactions	The FATF defines peer-to-peer transactions as VA transfers conducted without the use or involvement of a VASP or other obliged entity (such as VA transfers between two unhosted wallets whose users are acting on their own behalf). P2P transactions are not explicitly subject to anti-money laundering/countering the financing of terrorism (AML/CFT) controls under the FATF Standards. This is because the standards generally place obligations on intermediaries rather than on individuals themselves (with some exceptions, such as requirements related to implementing targeted financial sanctions).
Miners	Miners are participants in a decentralized virtual asset network who validate transactions and maintain the ledger by solving complex algorithms using special software. They are rewarded with newly created virtual assets or transaction fees for their work. While miners are not always directly involved in customer-facing services, they can pose ML/TF risks, especially when operating in anonymous mining pools or when rewards are distributed across opaque structures. These setups can be exploited to obfuscate the origin of illicit funds, facilitate layering, or process proceeds from ransomware or fraud schemes.
Mixers	Virtual asset mixers, also known as "tumblers" or "crypto mixers," are services that obfuscate the origin and destination of digital assets, making it difficult to trace the flow of funds. They achieve this by pooling funds from multiple users, mixing them, and then redistributing them to new addresses. This process obscures the connection between the original sender and recipient, enhancing anonymity.
Noncustodial (Cold) Wallet	A noncustodial (cold) wallet is a virtual asset wallet that provides users with complete control over their private keys and assets, while storing those keys offline for enhanced security. Unlike Custodial Wallets, users, rather than a third party, manage their keys and funds, reducing the risk of theft or loss due to third-party failures or hacks.
Perceived Threat	Refers to the level of ML/TF threat based on assessments, expert judgment, or credible open-source information in the absence of confirmed incidents. It involves threats that are reasonably assumed but not yet substantiated through formal evidence.

Politically Exposed Persons (PEPs)	<p><i>Foreign PEPs</i> are individuals who are or have been entrusted with prominent public functions by a foreign jurisdiction—for example, heads of state or of government; senior politicians; senior government, judicial, or military officials; senior executives of state-owned corporations; and important political party officials.</p> <p><i>Domestic PEPs</i> are individuals who are or have been entrusted domestically with prominent public functions—for example, heads of state or of government; senior politicians; senior government, judicial, or military officials; senior executives of state-owned corporations; and important political party officials.</p> <p><i>Individuals who are or have been entrusted with a prominent function by an international organization</i> refers to members of senior management—that is, directors, deputy directors, and members of the board or equivalent functions.</p> <p>The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.</p>
Privacy Coin	Privacy coins are a type of virtual asset designed to enhance user anonymity and transaction details, making them difficult to trace, unlike traditional cryptocurrencies which often have transparent public ledgers.
Residual Risk	Residual risk reflects the level of ML and TF risk after considering applicable mitigation measures. It adjusts the inherent risk score based on legislative and regulatory measures and their implementation by competent authorities and VASPs.
Stablecoin	This is a virtual asset whose value is pegged, or tied, to a stable asset, most often a fiat currency like the US dollar, but they can also be pegged to other assets like gold or a basket of currencies. This peg aims to minimize price volatility, making them a more reliable option than other virtual assets for everyday transactions and as a store of value within the VA ecosystem.
VA Payment Providers	These individuals are any natural or legal person who is not covered elsewhere under national legislation and, as a business, conducts the transfer of virtual assets for or on behalf of another natural or legal person.
VA-to-Fiat Exchange	This is the exchange between virtual assets and fiat currencies for or on behalf of another natural or legal person.
Virtual Asset ATMs	Virtual asset ATMs, also known as cryptocurrency or Bitcoin ATMs, are internet-connected kiosks that facilitate the exchange of fiat currency (like US dollars) for virtual assets (like Bitcoin) or vice versa. These machines are not traditional ATMs but rather a way to access the virtual asset market directly. They are operated by third-party companies, and users typically need a virtual asset wallet to receive or send funds.
Virtual Asset Casinos	A virtual asset casino is an online gambling platform that allows users to wager on casino games using virtual assets like Bitcoin, Ethereum, or others. These casinos offer a range of games and gambling services, similar to traditional online casinos, and typically provide features like quick deposits, withdrawals, and, in some cases, anonymity due to the use of blockchain technology.

Virtual Asset Over-the-Counter (OTC) Services	Virtual asset OTC services are a type of service that facilitates large trades of virtual assets, often between institutional clients, outside of traditional cryptocurrency exchangers. These services offer a way to execute large trades without disrupting market prices on exchangers.
Virtual Asset Staking	Virtual asset staking is a process in which investors deposit their virtual assets, like cryptocurrencies, on a platform to earn rewards, often interest. These rewards are typically paid in the same virtual asset that was staked. Essentially, investors contribute to the validation process of a blockchain network, and, in return, they receive a share of the network's rewards.
Wallet Providers	These individuals are any natural or legal person who is not covered elsewhere under national legislation and, as a business, conducts safekeeps and/or administers virtual assets or instruments enabling control over virtual assets for or on behalf of another natural or legal person.



6. Related FATF Documents

FATF (Financial Action Task Force). *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*. FATF, 2012–25. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>.

FATF. “Virtual Currencies: Key Definitions and Potential AML/CFT Risks.” FATF, June 2014. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html>.

FATF. “Professional Money Laundering.” FATF, July 2018. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Professional-money-laundering.html>.

FATF. “Public Statement on Virtual Assets and Related Providers. News release, June 21, 2019. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Public-statement-virtual-assets.html>.

FATF. *Guidance on Digital Identity*. FATF, 2020. <https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html>.

FATF. “Best Practices on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery.” FATF, October 2020. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Bestpracticesonconfiscationrecommendations4and38andaframeworkforongoingworkonassetrecovery.html>.

FATF. “Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets.” FATF, 2020. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html>.

FATF. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF, 2021. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>.

FATF. “Status of Implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity.” FATF, March 2024. <https://www.fatf-gafi.org/en/publications/Virtualassets/VACG-Snapshot-Jurisdictions.html>.

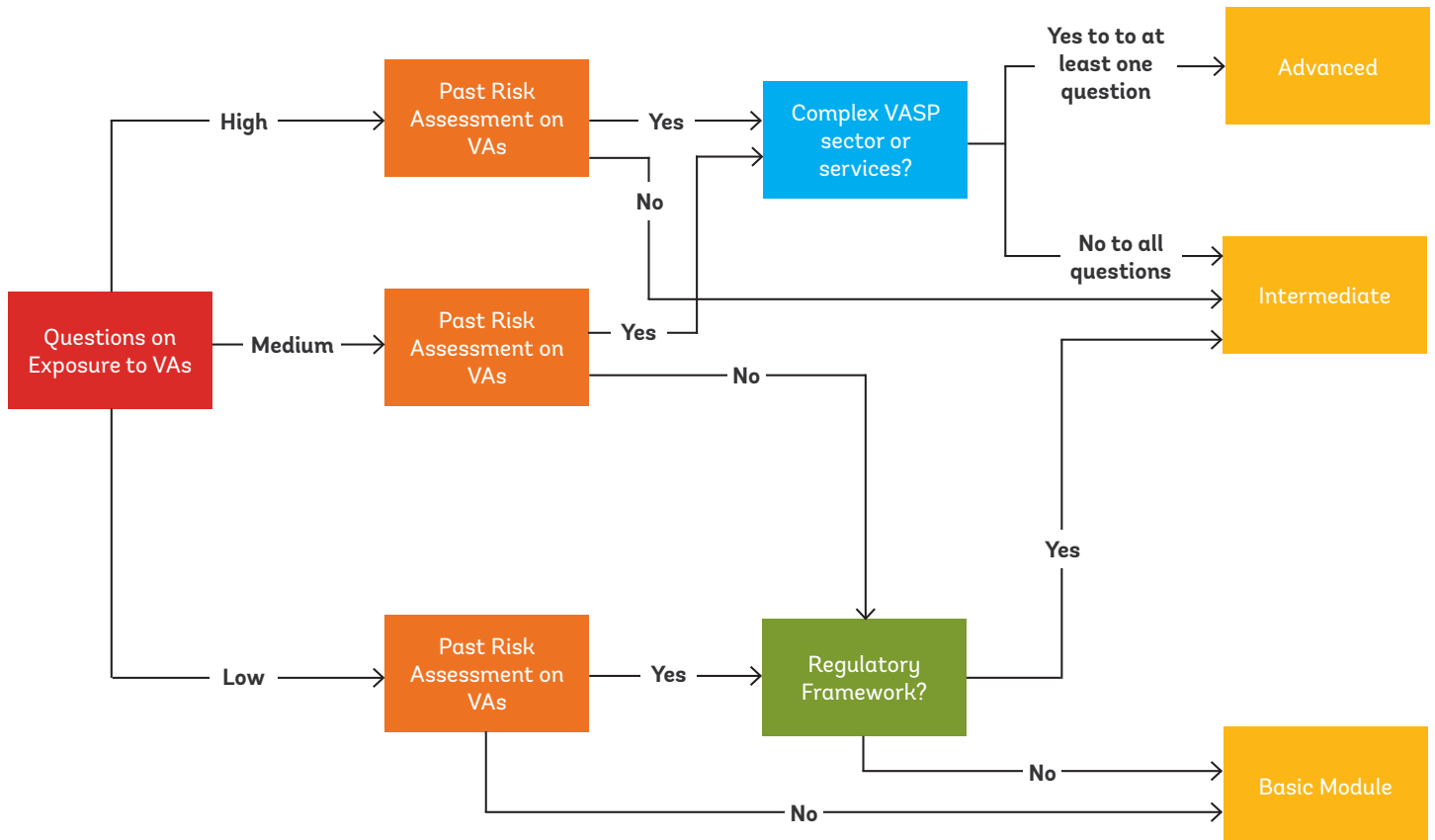
FATF. *Methodology for Assessing Technical Compliance with the FATF Recommendations and Effectiveness of AML/CFT/CPF Systems*. FATF, 2025. <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html>.

FATF. “Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs.” FATF, 2025. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html>.

Mutual evaluations and follow-up reports, 2018–present. Available at <https://www.fatf-gafi.org/en/publications/Mutualevaluations.html>.



ANNEX 1. Decision Tree for Tier Selection Quiz





ANNEX 2. Examples Illustrating ML/TF Techniques

This annex is designed to support the working group in filling the tab “ML & TF Techniques.”

	Technique	Description	Examples	News example
New obfuscation techniques that rely on unique characteristics of VA and distributed ledger technology				
1	Chain hopping/ cross-chain laundering	Rapidly swapping crypto between blockchains	ETH → USDT on Tron → BNB on Binance Smart Chain	After the \$540 million Ronin bridge hack in April 2022, the Lazarus Group moved stolen ETH through Tornado Cash and across multiple chains (Ethereum → Tron → BSC), obscuring the trail. ^a
2	Mixing/ tumbling services	Crypto pooled and redistributed to obscure transaction trails	Using Tornado Cash to hide Bitcoin movements	US Treasury sanctioned Tornado Cash in August 2022 for laundering over \$7 billion—including \$455 million stolen by North Korea’s Lazarus Group—through its Ethereum mixer. ^b
3	Use of privacy coins	Use of cryptocurrencies with privacy features	Converting Bitcoin to Monero (XMR)	In 2022, Ilya Lichtenstein and Heather Morgan were arrested in New York for laundering \$4.5 billion of stolen Bitcoin—partly by converting funds into Monero (XMR) to exploit its anonymity. ^c
4	Use of P2P exchangers	Direct crypto trades between users without KYC	Using Binance P2P to cash out illicit crypto	Reuters revealed North Korea’s Lazarus Group used Binance P2P (and other exchangers) to cash out stolen funds, exploiting minimal KYC at the time. ^d
5	Use of privacy wallets with built-in mixing features	Wallets that automatically obfuscate transaction details	Samourai Wallet’s Whirlpool service mixing transaction paths	Tornado Cash and Wasabi Wallet used for laundering; sanctioned by US Treasury. ^e
6	Use of OTC brokers	Conducting private crypto deals with little oversight	Selling Bitcoin for cash via an unregulated OTC desk	The UK’s “Operation Destabilise” uncovered OTC desks (Smart, TGR) laundering cartel and espionage proceeds via tether, leading to 84 arrests and £20 million seized. ^f

7	Use of stealth public key (addresses)	Conceals recipient identity via one-time addresses	Monero generating a new address for every transaction	Monero is using stealth addresses. ^g
8	Investment in virtual real estate	Using metaverse platforms to launder through land/property sales	Buying and flipping plots on Decentraland	Chainalysis reported that stolen funds from the Axie Infinity hack were laundered into Decentraland land parcels, then flipped for clean ETH. ^h
9	Sending dusting transactions	Small traceable transfers to track wallet behavior	Sending 0.00001 BTC to multiple wallets to deanonymize	DeFi web apps block users hit by Tornado Cash “Dust Attack.” ⁱ
10	Use of stablecoins on opaque blockchains	Avoid detection using hard-to-trace stablecoin networks	Transferring USDT via TRON (TRC-20) instead of Ethereum	Tornado Cash used to launder stolen funds including via USDC. ^j
11	Synthetic assets in DeFi	Moving value via synthetic tokens instead of actual assets	Swapping to sUSD or renBTC on DeFi platforms	US Treasury warned in April 2023 that criminal actors are using DeFi synthetic-asset platforms (synths) to layer illicit funds across multiple collateral types. ^k
12	Use of escrow/smart contracts	Splits or delays payments to hinder tracing	Smart contracts holding crypto before slow disbursement	Silo Finance hack via smart contract vulnerability; ~\$545K lost. ^l
13	Use of layer 2 networks	Moving funds on off-chain solutions to reduce traceability	Using the Lightning Network to transfer Bitcoin quickly	After the 2022 Ronin hack, attackers used the Lightning Network and Polygon’s layer-2 bridges to move stolen Bitcoin and ETH with reduced traceability. ^m
14	Token wrapping/unwrapping	Masks asset origin by reformatting tokens	Wrapping ETH into WETH before transferring	Wrapped tokens like WBTC used in cross-chain transactions and liquidity bridges; privacy and laundering risks persist. ⁿ
15	Use of DeFi protocols	Moving funds through decentralized finance to blur ownership	Lending dirty assets on Aave or Compound	A Chainalysis study found that 97% of hack proceeds in Q1 2022 were laundered through DeFi protocols (DEXs, bridges), marking a surge in layering via decentralized platforms. ^o

16	Use of DeFi liquidity pools	Blends illicit funds with legitimate assets	Depositing dirty funds into Uniswap pools	Railgun and Tornado Cash used to anonymize large flows of funds in DeFi protocols. ^p
Traditional obfuscation techniques that criminals and terrorists have adapted for the VA sector				
17	Opening wallets with fake/synthetic IDs	Using fraudulent documents to create accounts	Creating Binance account using AI-generated identity	Technique noted by law enforcement, but no prominent public cases. ^q
18	Opening wallets via shell companies	Hides owner identity through legal entities	Registering exchange account under a Seychelles-based LLC	"Operation Destabilise" uncovered crypto laundering via offshore entities. ^r
19	Use of domestic noncompliant VASPs	Transfers through unregulated local exchangers or ATMs	Using unregistered crypto ATM in a convenience store	Samourai Wallet operators were arrested for noncompliant mixing services. ^s
20	Use of foreign noncompliant VASPs	Sends funds via offshore unregulated platforms	Using a Russia-based exchanger that lacks KYC	OFAC sanctioned Tornado Cash for laundering over \$7 billion. ^t
21	Use of gambling platforms	Washing funds through crypto casinos or betting sites	Betting crypto at an online casino and cashing out as "winnings"	A U.N. report noted that Philippine casinos/junket operators laundered \$81 million stolen in the 2016 Bangladesh Bank hack, using gambling wins as cover. ^u
22	Structuring/smurfing	Breaking large transactions into smaller ones to avoid detection	10 deposits of \$900 each instead of \$9,000	Criminals used three different crypto ATMs—each capped at \$5,000/day—to "smurf" \$15,000 in small deposits across machines, effectively layering illicit cash without triggering alerts. ^v
23	Using VA proceeds for high-value purchases	Launders funds via real estate, art, and so on	Buying NFTs or apartments with illicit crypto	Criminal networks used crypto to fund luxury lifestyles via high-ticket items. ^w
24	Trading at inflated prices	Wash trades to disguise true transaction value	Selling a token for 10 times market price between wallets	NFT wash trading used to inflate value and launder funds; reported by Chainalysis. ^x

25	Use of gift cards	Converting crypto into gift cards and reselling for fiat	Buying Amazon gift cards with Bitcoin and selling them	Seven people in NYC were charged in a \$20 million gift-card scheme—they bought cards with illicit proceeds and immediately drained/resold them for fiat. ^y
26	Use of prepaid crypto cards	Loading crypto onto cards and spending like fiat	Spending dirty Bitcoin via a crypto Visa card	A DOJ indictment in 2023 charged operators of a crypto-prepaid card scheme that let users load illicit Bitcoin onto Visa-branded cards for instant spending. ^z
27	Employment of crypto mules	Using third parties to transfer crypto, breaking transaction links	Hiring mules to transfer crypto through multiple wallets	US prosecutors indicted dozens of “crypto mules” in 2022 who moved stolen funds through multiple accounts on behalf of hackers. US Department of Justice. ^{aa}
28	Comingling funds in a VASP	Mixes illicit with legitimate funds in wallets	Blending stolen crypto with staking rewards	Tornado Cash commingled illicit and legitimate funds, making tracing nearly impossible. ^{ab}
Techniques used specifically for generating criminal proceeds in virtual assets				
29	Ransomware payments	Laundering ransomware proceeds through crypto mixing and swapping	Using Monero after a ransomware attack	The DOJ seized \$2.3 million in Bitcoin that Colonial Pipeline paid to the DarkSide ransomware gang—recovering 63.7 BTC days after the May 2021 hack. ^{ac}
30	Fraudulent investment platforms	Fake schemes lure victims to send crypto	Fake DeFi yield farm promising 50% weekly returns	OneCoin Ponzi scheme defrauded investors of billions globally. ^{ad}
31	Social engineering scams	Tricks victims into transferring assets	Romance scammer requesting Bitcoin “to escape warzone”	Lazarus Group “TraderTraitor” phishing attacks used LinkedIn to target crypto employees. ^{ae}
32	Hacking exchangers/ wallets	Steals funds through cyberattacks	Breach of exchange hot wallets (for example, Mt. Gox)	Multiple hacks in 2024–2025 including Bybit (\$1.5 billion), Binance (\$40 million), and Iran-based exchanger (\$90 million). ^{af}
33	Fraudulent QR codes on ATMs	Replaces QR codes to redirect funds	Sticking fake QR codes on public Bitcoin ATMs	Warnings for this technique appear online, despite no major publicly known cases available. ^{ag}

34	Insider abuse within VASPs	Employees siphon customer assets	Exchanger staff redirecting withdrawals to own wallet	Lazarus-linked hacks exploited legitimate employee credentials in exchangers. ^{ah}
35	Cryptojacking	Hijacks computers to secretly mine crypto	Malware installed to mine Monero in background	Coinhive Monero miner embedded in Starbucks Wi-Fi and websites. ^{ai}
36	Flash loan attacks	Exploiting DeFi flash loans to wash or move stolen funds	Flash loan attack on a DeFi protocol followed by rapid fund movement	The first major flash-loan exploit hit bZx in February 2020, using an undercollateralized short position via a flash loan to net over \$350,000. ^{aj}
Techniques specific to terrorist financing				
37	Terrorist financing via crowdfunding	Collects donations through crypto-enabled campaigns	Extremist group asking for BTC donations via Telegram	There is some available reporting on mixing services used for terror-related activities. ^{ak}
38	Sale of NFTs for extremist causes	Funds terrorism via NFT purchases	Selling propaganda-themed NFTs on obscure marketplaces	NFT marketplaces flagged for abuse, but no clear examples of extremist fundraising found in recent mainstream reporting. ^{al}

Note: BNB = Binance; BTC = Bitcoin; DOJ = US Department of Justice; ETH = Ether; ID = identification; LLC = limited liability company; OFAC = Office of Foreign Assets Control; Q1 = first quarter; UK = United Kingdom; USDT = Tether; WBTC = wrapped Bitcoin; WETH = wrapped Ethereum; XMR = Monero.



Notes

1. This guidance uses the following Financial Action Task Force definition of a virtual asset: “a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. VAs do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations” (FATF Standards, as of 2025).
2. Nikou Asgari, “Global Crypto Assets Hit \$4tn as Industry Wins Backing of US Lawmakers,” Financial Times, July 18, 2025, <https://www.ft.com/content/3f503b72-6cb5-4002-813c-57d53590635e?>.
3. This guidance aligns with the FATF definition of a virtual asset service provider (VASP), which is the following: “any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset” (FATF Standards, as of 2025).
4. For an overview of key AML/CFT terms, please refer to the glossary at the end of this document.
5. See the OECD’s Crypto Asset Reporting Framework; FSB’s High-Level Recommendations for the Regulation, Supervision, and Oversight of Crypto-asset Activities and Markets; and United Nations Security Council Resolution 2462 of March 28, 2019, among others.
6. Bitcoin is a decentralized digital currency used for encrypted, peer-to-peer transactions without needing a central bank. It was created by Satoshi Nakamoto, a pseudonymous person or team who outlined the technology in a 2008 white paper.
7. Ethereum is a decentralized, blockchain-based public software platform that facilitates peer-to-peer contracts and decentralized applications (dApps). Its native cryptocurrency, Ether (ETH), is used to power transactions and run smart contracts on the platform. It can be thought of as a global computer that runs programs, including smart contracts, without a central authority.
8. Monero is a privacy coin. Privacy coins are a type of virtual asset designed to enhance user anonymity and transactions details, making them difficult to trace, unlike traditional cryptocurrencies which often have transparent public ledgers.
9. Tether is a stablecoin pegged primarily to the US dollar and designed to maintain a 1:1 value ratio.
10. USD Coin is a fully backed stablecoin pegged to the US dollar.
11. DAI is a decentralized, crypto-collateralized stablecoin pegged to the US dollar.

12. Basic Attention Token is a utility token designed to improve digital advertising efficiency by rewarding users for their attention while providing advertisers with better targeting.
13. Chainlink is a decentralized oracle network that provides real-world data to smart contracts on blockchain platforms.
14. A non-fungible token is a digital asset representing unique ownership of a specific item, whether digital or physical (such as art or media), on a blockchain. Unlike fungible assets like currency (in which each unit is identical and interchangeable), NFTs are distinct and cannot be exchanged for another on a one-to-one basis.
15. CBDCs are digital forms of a jurisdiction's fiat currency issued and regulated by the central bank.
16. These are digital tokens or assets issued by companies as rewards or for use within specific platforms (such as gaming environments).
17. Tokenized deposits are digital representations of traditional bank deposits issued on blockchain platforms.
18. For such jurisdictions, the tool provides an option to select “not applicable” or “unknown” for certain questions on the strength of domestic AML/CFT regulation, for example.
19. Decentralized finance refers to financial services provided through arrangements that use smart contracts on distributed ledgers (blockchain technology), enabling peer-to-peer transactions without relying on traditional financial intermediaries.
20. Platform-issued tokens are digital tokens created and distributed by a specific blockchain-based platform or project. They can serve various purposes such as access to services, staking, rewards, or use within the platform's ecosystem.
21. Governance tokens are a type of cryptocurrency that grants holders voting rights on protocol decisions, upgrades, or changes in decentralized organizations or platforms. The tokens are central to decentralized governance models such as decentralized autonomous organizations (DAOs).
22. Specifically, the risk assessment tool factors in the general national vulnerabilities by evaluating the effectiveness of mitigation measures and the level of threats. For example, for jurisdictions that indicate they have a high level of corruption, the tool automatically reflects this by slightly reducing the impact of mitigation measures.
23. A reason for not including a domestic versus foreign distinction for decentralized financial services is that the geographic location of such services is often very challenging to determine.
24. Such cases can include: the creation of fake crypto mining operations, Ponzi or pyramid schemes involving funding for crypto mining, or cryptojacking—theft of processing power often at a large scale to mine crypto assets.
25. For jurisdictions that are completing the basic and intermediate modules, the output charts will show only those categories that are being assessed.
26. Notably, the extent to which DeFi services fall under the FATF definition of a VASP will depend on the level of ownership and control of the platform (that is, whether a natural or legal person has control over the platform) and whether the service is being offered for, or on behalf of, another individual.
27. Financial Action Task Force, “Stocktake on Data Pooling, Collaborative Analytics and Data Protection (FATF, 2021).

- a. TRM Labs, "North Korea's Lazarus Group Moves Funds Through Tornado Cash," TRM Blog, April 27, 2022, <https://www.trmlabs.com/resources/blog/north-koreas-lazarus-group-moves-funds-through-tornado-cash>.
- b. Hannah Lang, "US Scraps Sanctions on Tornado Cash, Crypto 'Mixer' Accused of Laundering North Korea Money," Reuters, March 21, 2025, <https://www.reuters.com/business/finance/us-scraps-sanctions-tornado-cash-crypto-mixer-accused-laundering-north-korea-2025-03-21>.
- c. Andy Greenberg, "The DOJ's \$3.6B Bitcoin Seizure Shows How Hard It Is to Launder Crypto," Wired, February 9, 2022, <https://www.wired.com/story/bitcoin-seizure-record-doj-crypto-tracing-monero>.
- d. Angus Berwick and Tom Wilson, "How Crypto Giant Binance Became a Hub for Hackers, Fraudsters and Drug Traffickers," Reuters special report, June 6, 2022, <https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirtymoney>.
- e. Adam Hayes, "CoinJoin: What It Is, How It Works, and Privacy Considerations," Investopedia, updated July 21, 2024, <https://www.investopedia.com/terms/c/coinjoin.asp>.
- f. Miles Johnson and Suzi Ring, "UK Uncovers Vast Crypto Laundering Scheme for Gangsters and Russian Spies," Financial Times, December 4, 2024, <https://www.ft.com/content/31b9053f-343e-4c47-ace9-2b0080ec8799>.
- g. Monero, "Stealth Address," Moneropedia, accessed August 20, 2025, <https://www.getmonero.org/resources/moneropedia/stealthaddress.html>.
- h. Elliptic, "North Korea's Lazarus Group Identified As Exploiters Behind \$540 Million Ronin Bridge Heist," Elliptic Intel, updated April 14, 2022, <https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge>.
- i. Sebastian Sinclair and David Canellis, "DeFi Web Apps Block Users Hit by Tornado Cash 'Dust Attack'," Blockworks, August 15, 2022, <https://blockworks.co/news/defi-web-apps-block-users-hit-by-tornado-cash-dust-attack>.
- j. Elliptic, "Tornado Cash Mixer Sanctioned after Laundering over \$1.5 billion," Elliptic, August, 8 2022, <https://www.elliptic.co/blog/analysis/tornado-cash-mixer-sanctioned-after-laundering-over-1-5-billion>.
- k. Reuters, "U.S. Says Decentralized Finance Services Being Used for Illicit Transfers," Reuters, April 6, 2023, <https://www.reuters.com/technology/us-says-decentralized-finance-services-being-used-illicit-transfers-2023-04-06>.
- l. News Feeder, "Vitalik Buterin's Stealth Addresses: A Game-Changer for Ethereum Privacy Amid DeFi Security Concerns," OKX United States, Jun 27, 2025, <https://www.okx.com/en-us/learn/vitalik-stealth-addresses-ethereum-privacy>.
- m. Arda Akartuna, "Top five DeFi crime trends of 2022," Elliptic blog, December 15, 2022, <https://www.elliptic.co/blog/analysis/top-five-defi-crime-trends-of-2022>.
- n. Joel Khalili, "A New Crypto Mixer Promises to Be Tornado Cash without the Crime," Wired, March 3, 2023, <https://www.wired.com/story/new-crypto-mixer-promises-to-be-tornado-cash-crime/>.
- o. Chainalysis Team, "Hackers Are Stealing More Cryptocurrency from DeFi Platforms Than Ever Before," Chainalysis, April 14, 2022, <https://www.chainalysis.com/blog/2022-defi-hacks>.

- p. Simon Brown, "Privacy in Ethereum—Stealth Addresses," Medium, November 21, 2024, <https://simbro.medium.com/privacy-in-ethereum-stealth-addresses-f05016109010>.
- q. Emma McGowan, "What Is Synthetic Identity Theft and How Does It Work?," LifeLock by Norton, updated November 28, 2024, https://lifelock.norton.com/learn/identity-theft-resources/synthetic-identity-theft?srsId=AfmBOopkXiW-xxJjQU_mEck6MrljAPVhkVqRM_zJbWxjzMCf5mRgG5I6.
- r. Matt Burgess, "She Was a Russian Socialite and Influencer. Cops Say She's a Crypto Laundering Kingpin," Wired, December 4, 2024, <https://www.wired.com/story/operation-destabilise-money-laundering/>.
- s. US Attorney's Office, Southern District of New York, "Founders and CEO of Cryptocurrency Mixing Service Arrested and Charged with Money Laundering and Unlicensed Money Transmitting Offenses," press release, April 24, 2024, <https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering>.
- t. US Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," press release, August 8, 2022, <https://home.treasury.gov/news/press-releases/jy0916>.
- u. Tom Wilson, "North Korean Hackers, Criminals Share Money Laundering Networks in Southeast Asia—UN Report," Reuters, January 15, 2024, <https://www.reuters.com/world/asia-pacific/north-korean-hackers-criminals-share-money-laundering-networks-southeast-asia-un-2024-01-15/>.
- v. Thomson Reuters Institute, "Cryptocurrency ATMs: Risks, Rewards and Getting to Know Your Customers," April 22, 2022, Thomson Reuters Institute, <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/cryptocurrency-atms>.
- w. Burgess, "She Was a Russian Socialite and Influencer."
- x. Chainalysis Team, "Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering in This Emerging Asset Class," Chainalysis blog post, February 2, 2022, <https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/>.
- y. Joseph Wilkinson, "7 people charged in \$20 million gift card scam based in NYC," New York Daily News, March 6, 2025, <https://www.yahoo.com/news/7-people-charged-20-million-204900714.html>.
- z. US Department of Justice, "Operators of Cryptocurrency Mixers Charged with Money Laundering," press release, January 10, 2025, <https://www.justice.gov/archives/opa/pr/operators-cryptocurrency-mixers-charged-money-laundering>.
- aa. US Department of Justice, "Two Arrested for Alleged Conspiracy to Launder \$4.5 Billion in Stolen Cryptocurrency," press release, February 8, 2022, <https://www.justice.gov/archives/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency>.
- ab. US Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," press release, August 8, 2022, <https://home.treasury.gov/news/press-releases/jy0916>.
- ac. Christopher Bing, Joseph Menn, and Sarah N. Lynch, "U.S. Seizes \$2.3 Mln in Bitcoin Paid to Colonial Pipeline hackers," Reuters, June 7, 2021, <https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07>.

- ad. US Attorney's Office, Southern District of New York, "OneCoin Was a Fraudulent Cryptocurrency Marketed and Sold to Millions of Victims Around the World, Resulting in Billions of Dollars in Losses," press release, September 12, 2023, <https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison>.
- ae. Cybersecurity and Infrastructure Security Agency (CISA), "TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies," cybersecurity advisory, April 20, 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a>.
- af. Crystal Investigations Team, "The 10 Biggest Crypto Hacks in History," Crystal Investigations, April 2, 2025, <https://crystalintelligence.com/investigations/the-10-biggest-crypto-hacks-in-history/>.
- ag. Iowa State Bank, "Bitcoin ATM Scams on the Rise," Iowa State Bank blog, April 2, 2025, <https://www.iowastate.bank/blog/post/bitcoin-atm-scams-on-the-rise#:~:text=They%20may%20text%20you%20a.%2C%20or%20computer%20pop%20Dups>.
- ah. Ionut Alexandru Baltariu, Andrei Anton-Aanei, and Alina Bîzgă, "Lazarus Group Targets Organizations with Sophisticated LinkedIn Recruiting Scam," Bitdefender blog post, February 05, 2025, <https://www.bitdefender.com/en-us/blog/labs/lazarus-group-targets-organizations-with-sophisticated-linkedin-recruiting-scam>.
- ai. Leo Kelion, "Starbucks Cafe's Wi-Fi Made Computers Mine Crypto-Currency," BBC, 13 December 13, 2017, <https://www.bbc.com/news/technology-42338754>.
- aj. AON, "Flash Loan Attacks: A Case Study," blog post, October 13, 2023, <https://www.aon.com/en/insights/cyber-labs/flash-loan-attacks-a-case-study>.
- ak. Financial Action Task Force (FATF), "Crowdfunding for Terrorism Financing," FATF Report, 2023, <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf>.
- al. US Department of the Treasury, "Treasury Releases First Ever Non-Fungible Token Illicit Finance Risk Assessment," press releases, May 29, 2024, <https://home.treasury.gov/news/press-releases/jy2382#:~:text=The%20report%20determines%20that%20illicit,contrast%20to%20fraudsters%2C%20to%20date>.

