STRATEGY

EU AML / CFT
GLOBAL FACILITY

EU GLOBAL FACILITY METHODOLOGY ON VIRTUAL ASSETS

COMPREHENSIVE AML/CFT FRAMEWORK

FEBRUARY 2026

Funded by the European Union

EXPERTISE FRANCE
GROUPE AFD

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Disclaimer:
This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the EU Global Facility on AML/CFT and do not necessarily reflect the views of the European Union.

For further information, please contact:
info@global-amlcft.eu
www.global-amlcft.eu

EU AML / CFT
GLOBAL FACILITY

Table of Contents

Acronyms

AML/CFT	Anti-Money Laundering and Counter the Financing of Terrorism
EU Global Facility	EU Global Facility on AML/CFT
FATF	Financial Action Task Force
DeFi	Decentralised Finance
DPRK	Democratic People's Republic of Korea
NFT	Non-Fungible Tokens
OSINT	Open-source intelligence
VAs	Virtual Assets
VASPs	Virtual Assets Service Providers

Executive Summary

The virtual asset ecosystem has undergone profound transformation since the Financial Action Task Force (FATF) first addressed cryptocurrency risks in 2014. What began as a niche technology has evolved into a complex financial ecosystem encompassing not only traditional cryptocurrencies but also stablecoins, decentralised finance protocols, non-fungible tokens, and cross-chain bridges. This evolution demands a corresponding advancement in regulatory frameworks and supervisory methodologies.

The EU Global Facility on Anti Money Laundering and Countering the Financing of Terrorism (hereafter referred to as "EU Global Facility") recognises that effective regulation of virtual assets requires a comprehensive approach that addresses both traditional centralised exchanges and the emerging decentralised ecosystem. This comprehensive framework[1] provides countries with practical tools and guidance to assess risks, implement supervision, conduct investigations, and manage seized assets across the full spectrum of virtual asset activities.

[1] A first version of this methodology was published in April 2023

EU AML/CFT
GLOBAL FACILITY

EU GLOBAL FACILITY

METHODOLOGY ON VIRTUAL ASSETS

01

Strategic Decision

Guidance on the "Prohibition vs. Regulation" spectrum. Conducting diagnostic assessments, stakeholder consultations, and initial policy formulation.

02

Risk Assessment

Identification of ML/TF threats specific to the jurisdiction. Specialised modules for DeFi Stablecoins, and NFT market vulnerabilities.

03

VASP Supervision

Building capacity for licensing and ongoing monitoring. Development of supervision manuals and blockchain analytics training for regulators.

04

Investigation & Tracing

Equipping law enforcement with advanced tools. Cross-chain forensics, deanonymisation techniques, and attribution of illicit flows.

05

Seizure & Confiscation

Managing virtual assets from seizure to liquidation. Secure custody protocols, key management, and value realisation strategies.

06

Proliferation Financing

Countering state-sponsored sanctions evasion. Advanced attribution for DPRK/ Iran threats, mixer analysis, and counter-measures.

EU AML / CFT
GLOBAL FACILITY

INTRODUCTION

Funded by
the European Union

EU AML/CFT
GLOBAL FACILITY

Introduction: The Evolution of Virtual Assets

The cryptocurrency landscape has dramatically evolved beyond simple peer-to-peer electronic cash systems, as Satoshi Nakamoto wanted in his historical White Paper Bitcoin: Peer-to-Peer Electronic Cash System. Today's Virtual Assets (VAs) ecosystem encompasses diverse technologies and business models that present both opportunities for financial innovation and challenges for regulatory oversight. The rise of anonymity-enhanced cryptocurrencies, mixing services, decentralised exchanges, privacy wallets, and cross-chain bridges has created an environment where traditional regulatory approaches require substantial adaptation.

The emergence of decentralised finance protocols has fundamentally altered how financial services operate in the digital realm. These protocols enable lending, borrowing, trading, and yield generation without traditional intermediaries, creating regulatory challenges as no single entity controls these systems. Similarly, the explosion of non-fungible tokens has created new avenues for value transfer that may fall outside traditional virtual asset service providers (VASPs) definitions, while stablecoins have become the dominant medium for both legitimate commerce and illicit finance in the crypto ecosystem alike.

Given this rapid evolution, the FATF recognised the need for comprehensive standards that could adapt to technological innovation while maintaining effectiveness against money laundering and terrorist financing (ML/TF) risks. The global implementation of these standards ensures that virtual asset technologies can continue to innovate responsibly while preventing exploitation by criminals and terrorists seeking jurisdictions with weak supervision.

EU AML / CFT
GLOBAL FACILITY

Part 1: FATF's Regulatory Framework for Virtual Assets

Funded by
the European Union

EU AML/CFT
GLOBAL FACILITY

Part I: FATF's Regulatory Framework for Virtual Assets

Historical Development and Current Standards

The FATF's engagement with virtual assets began in June 2014 with the publication of "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," which represented the first systematic attempt to understand and categorise the money laundering and terrorist financing risks associated with cryptocurrency payment mechanisms. This initial framework established the foundation for understanding how value could be transmitted over the internet outside traditional financial systems.

The pivotal moment in virtual asset regulation came in October 2018 when the FATF adopted formal definitions for "virtual asset" and "virtual asset service provider". These definitions established that virtual assets constitute a digital representation of value that can be digitally traded or transferred and used for payment or investment purposes, explicitly excluding digital representations of fiat currencies and securities already covered by existing recommendations. VASPs were defined to encompass any natural or legal person conducting exchange services between virtual assets and fiat currencies, exchanges between different VAs, transfers of VAs, safekeeping and administration services, or participation in financial services related to initial coin offerings.

Recommendation 15 and Its Implementation

The 2019 amendment to FATF Recommendation 15 marked a watershed moment in virtual asset regulation, establishing that VASPs must be subject to the same anti-money laundering and counter-terrorist financing (AML/CFT) obligations as traditional financial institutions. This recommendation requires countries to ensure that VASPs conduct comprehensive customer due diligence, implement transaction monitoring systems, maintain records, and report suspicious activities to relevant authorities... etc.

The implementation of Recommendation 15 requires countries to establish licensing or registration requirements for VASPs operating within their jurisdiction. This includes requirements for appropriate governance structures, risk management systems, and internal controls that can effectively identify and mitigate ML/TF risks. The recommendation also emphasises the importance of international cooperation and information sharing, recognising that VAs operate across borders and require coordinated regulatory responses.

Countries implementing Recommendation 15 face the fundamental choice of whether to prohibit or regulate

VAs activities. Those choosing prohibition must still assess the risks associated with virtual assets and maintain tools and authorities to enforce the prohibition effectively. Countries opting for regulation must develop comprehensive frameworks that address the full range of virtual asset activities while remaining adaptable to technological innovation.

The Travel Rule and Cross-Border Challenges

The application of the Travel Rule to virtual asset transfers represents one of the most significant implementation challenges. This requirement mandates that virtual asset service providers obtain, hold, and transmit required originator and beneficiary information for transfers above designated thresholds. The technical implementation of this requirement has proven complex, requiring the development of new protocols and standards for information sharing between VASPs across different jurisdictions and technological platforms.

Implementation Challenges and Status (2024-2025)

The implementation of Recommendation 15 has been a major challenge for many countries, particularly those with emerging economies or weaker regulatory systems. The FATF's 2024 Targeted Update revealed that global implementation is still lagging significantly. As of 2024, 75% of jurisdictions were only partially or not compliant with the FATF's requirements, a statistic that has shown negligible improvement over previous years.

As of April 2025, 138 jurisdictions have been assessed for compliance with the FATF standards for VAs and VASPs and the data reflect ratings related to technical compliance with the FATF requirements, as set out in Recommendation 15 and its Interpretative Note. While the proportion of jurisdictions partially compliant with the revised Recommendation 15 remains similar (49%; 68 of 138 jurisdictions) to the results in 2024 (50%; 65 of 130 jurisdictions), global implementation has slightly improved. 29% of jurisdictions (40 of 138 jurisdictions) are now largely compliant with the FATF's requirements for VA/VASPs (25%; 32 of 130 jurisdictions in 2024). The proportion of jurisdictions not compliant with the requirements has decreased from 25% to 21%. There is only one country that achieved a compliant rating.

Decentralised Finance (DeFi) and Unhosted Wallets

The FATF has explicitly addressed the rise of DeFi and unhosted wallets. While "true" decentralisation might theoretically place a protocol outside the scope of VASP definitions, the FATF applies a "substance over form" approach. If a DeFi arrangement involves persons with control or sufficient influence over the protocol—such as holders of administrative keys or governance tokens—they may fall under the definition of a VASP and thus be subject to AML/CFT obligations. The EU Global Facility strategy emphasises that "decentralisation" is not a shield against regulation, and supervisors must be equipped to identify the centralised entities often hiding behind decentralised architectures.

EU AML / CFT
GLOBAL FACILITY

Part II: Strategic Decision Framework Prohibition VS Regulation

Funded by
the European Union

Part II: Strategic Decision Framework Prohibition VS Regulation

Understanding the Regulatory Spectrum

Countries approaching virtual asset regulation must carefully consider their position on the spectrum between complete prohibition and comprehensive regulation. This decision should be informed by thorough risk assessment, consideration of national (economic and social) circumstances, and evaluation of enforcement capacity. The choice is not merely binary; many jurisdictions adopt hybrid approaches that regulate certain activities while prohibiting others, or that phase in regulatory requirements over time as capacity develops.

The decision to regulate virtual assets offers several compelling advantages. Consumer protection mechanisms can prevent fraud and ensure that exchanges and wallet providers maintain appropriate security standards and operational resilience. AML/CFT requirements enable authorities to prevent criminal exploitation of virtual assets while preserving legitimate use cases. Taxation frameworks ensure that virtual asset transactions contribute appropriately to public revenues, addressing concerns about tax evasion through cryptocurrency transactions. Perhaps most importantly, clear regulatory frameworks can boost market confidence by providing legal certainty for businesses and investors operating in the virtual asset space.

Conversely, some jurisdictions have concluded that prohibition represents the most appropriate response to virtual asset risks. Concerns about criminal activity, including ML/TF, and ransomware payments, drive many prohibition decisions. The perceived lack of effective regulatory tools, combined with the volatility of virtual asset markets and environmental concerns about energy-intensive mining operations, leads some countries to conclude that the risks outweigh potential benefits. Other countries cite capital flight, e-dollarisation and destabilising exchange rates or bank exclusion as other purely economic reasons for the ban.

Implementation Considerations for Both Approaches

Countries choosing prohibition must recognise that declaring VAs illegal does not eliminate their use. Effective prohibition requires robust enforcement mechanisms, including the technical capacity to detect virtual asset transactions, legal frameworks that enable prosecution of violations, and international cooperation to address cross-border activities. The risk assessment requirement under Recommendation 15 applies equally to prohibiting countries, as understanding the risks is essential for effective enforcement.

For countries choosing regulation, the implementation journey requires a myriad of regulatory measures. Initial steps typically include establishing legal definitions and regulatory scope, followed by licensing or registration requirements for VASPs. As regulatory capacity develops, countries can implement more sophisticated requirements for transaction monitoring, suspicious activity reporting, and compliance with international standards such as the Travel Rule.

The resource requirements for either approach should not be underestimated. Prohibition requires investment in enforcement capacity, including training for law enforcement, prosecutors, and judges. Regulation demands the development of supervisory expertise, technological infrastructure for monitoring compliance, and ongoing engagement with a rapidly evolving industry. Both approaches benefit from public-private partnerships that leverage industry expertise while maintaining appropriate regulatory independence.

Options Beyond Binary Choice

While the debate is often framed as "ban or regulate," in reality, countries have adopted various intermediate approaches reflecting their specific circumstances and concerns. The EU Global Facility on AML/CFT assists countries in understanding the full spectrum of policy options.

Comprehensive regulation represents one end of the spectrum, involving full implementation of FATF recommendations with licensing or registration of all VASPs, comprehensive AML/CFT obligations comparable to traditional financial institutions, active supervision and enforcement, and enabling legal framework for VAs businesses. This approach is most suitable for countries with significant virtual asset activity, adequate regulatory capacity, desire to

foster innovation within a controlled framework, and commitment to sustained resource investment.

Restricted regulation represents a middle approach, involving permitting some virtual asset activities while prohibiting others. For example, a country might allow virtual asset exchange and custody services by licensed entities while prohibiting peer-to-peer exchange platforms or privacy-enhanced cryptocurrencies. This approach enables regulatory focus on specific higher-risk activities while limiting exposure to areas where supervision would be most challenging. The approach requires careful definition of permitted versus prohibited activities and enforcement against unauthorised activities.

Watch-and-wait represents another intermediate approach, involving temporary prohibition or restriction while building capacity and developing regulatory frameworks, active monitoring of virtual asset developments and risks, pilot programmes or regulatory sandboxes to test approaches, and eventual transition to either comprehensive regulation or longer-term prohibition based on experience. This approach suits countries facing significant uncertainty about risks and benefits, needing time to build institutional capacity, and wanting to learn from international experience before committing to a permanent approach.

Complete prohibition represents the other end of the spectrum, involving bans on all virtual asset activities including exchange, custody, mining, and usage for payments, penalties for violations, and blocking of access to foreign virtual asset platforms. This approach is most suitable for countries with minimal current virtual asset activity, capacity constraints for effective regulation, acute concerns about capital flight or currency stability.

Regulatory Approaches to Virtual Assets

THE POLICY SPECTRUM: FROM PROHIBITION TO COMPREHENSIVE REGULATION

01

Complete Prohibition

A total ban on all VAs activities, including exchange, custody, mining, and usage for payments.

KEY MEASURES
- Strict penalties for violations
- Blocking foreign platform access
- Ban on banking integration

BEST SUITED FOR
Countries with minimal VA activity, acute capital flight risks, or capacity constraints preventing effective regulation.

02

Watch & Wait

Temporary restriction or prohibition while building institutional capacity and monitoring market risks.

KEY MEASURES
- Regulatory sandboxes/Pilots
- Active risk monitoring
- Developing legal frameworks

BEST SUITED FOR
Jurisdictions facing uncertainty, needing time to learn from international experience before committing.

03

Restricted Regulation

A middle approach permitting specific activities (e.g., custody) while prohibiting higher-risk ones.

KEY MEASURES
- Ban on Privacy Coins/P2P
- Licensed custody & exchange
- Targeted vision focus

BEST SUITED FOR
Focusing resources on manageable risks while limiting exposure to areas where supervision is difficult.

04

Comprehensive Regulation

Full implementation of FATF standards with a complete licensing and supervisory regime.

KEY MEASURES
- Full AML/CFT obligations
- Active enforcement
- Fostering controlled innovation

BEST SUITED FOR
Countries with significant VA activity, high regulatory capacity, and resources for sustained investment.

Decision-Making Process and Stakeholder Engagement

The EU Global Facility guides countries through a structured decision-making process that ensures all relevant perspectives are considered and decisions are well-informed. This process typically involves multiple stages.

The initial diagnostic phase involves collecting baseline information about virtual asset activity, threats, and capacity. This includes surveys of financial institutions about their customers' virtual asset activity, interviews with law enforcement about criminal use of virtual assets, assessment of current legal framework regarding VAs status, evaluation of regulatory and supervisory capacity, and preliminary threat and risk identification. This diagnostic provides the factual foundation for subsequent analysis.

The stakeholder consultation phase ensures that diverse perspectives inform the decision. Key stakeholders include financial sector representatives who understand legitimate demand for virtual asset services and operational implications of different approaches, law enforcement and prosecutors who understand criminal exploitation of virtual assets and enforcement feasibility, Structured consultations through workshops, Open-source intelligence (OSINT) work, written submissions, and advisory committees enable countries to understand implications of different approaches from multiple angles.

The EU Global Facility provides facilitation, methodological guidance, and international best practice examples to support this analysis. Countries examine each dimension thoroughly, documenting their findings and reasoning. This analysis often reveals that the optimal approach is not obvious but involves trade-offs between competing considerations. The analytical phase produces a comprehensive report documenting the analysis and presenting options with their respective advantages, disadvantages, and implementation requirements.

The EU Global Facility does not advocate for particular outcomes but ensures that decision-makers have clear, comprehensive information to inform their choices. Decisions should be documented in policy statements or strategic plans that provide transparency about the rationale and intended approach.

Supporting Regional Coordination

Virtual assets do not respect national borders, making regional coordination valuable for enhancing effectiveness and reducing harmful regulatory arbitrage. The EU Global Facility facilitates regional dialogues where countries can discuss their approaches, share experiences, and identify opportunities for coordination. Regional coordination can involve harmonised regulatory frameworks that reduce compliance costs for businesses operating across multiple countries, mutual recognition of licensing for VASPs operating regionally, coordinated supervisory colleges for regional VASP groups, information sharing agreements for cross-border enforcement, joint training and capacity-building initiatives, and coordinated public awareness campaigns.

Regional approaches are particularly valuable where countries within a region have close economic integration, significant cross-border movement of people and capital, shared infrastructure such as payment systems, and similar legal traditions facilitating regulatory harmonisation. The EU Global Facility has supported regional dialogues, conducted usually through FATF-Style Regional Bodies, in multiple regions, enabling countries to learn from each other's experiences and develop coordinated approaches that enhance collective effectiveness while respecting national sovereignty.

Linking to Other Pillars

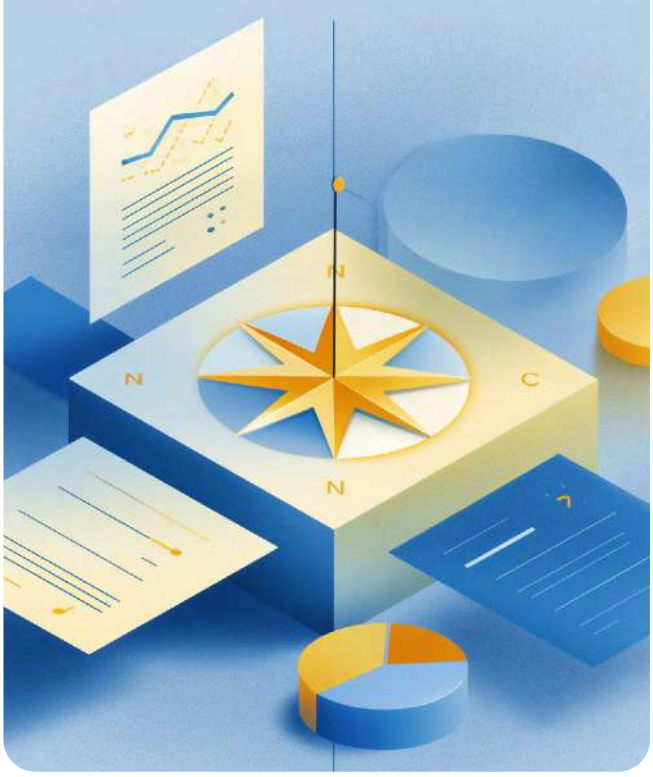
The strategic decision on whether to ban or regulate virtual assets fundamentally shapes how countries engage with the other five pillars of the EU Global Facility framework. Countries choosing prohibition approaches still need capability for risk assessment to understand evolving threats, investigation and tracing to detect prohibited activity and prosecute violators, seizure and confiscation to deprive violators of illicit proceeds, and attention to proliferation financing and sanctions evasion which may occur through virtual assets despite prohibition. However, the supervision pillar becomes less relevant under prohibition, while enforcement against unauthorised activity becomes paramount.

Countries choosing regulatory approaches need comprehensive engagement with all six pillars, including risk assessment to inform supervisory priorities and regulatory adjustments, VASP supervision as the core mechanism for ensuring compliance, investigation and tracing to address criminal misuse despite regulation, seizure and confiscation for enforcement and asset recovery, and proliferation financing, sanctions evasion, and emerging threat response. The strategic decision therefore establishes the foundation upon which the entire virtual asset framework is built.

Strategic Decision Support

Guidance on the "Prohibition vs. Regulation" spectrum

- Diagnosis assessments of national VA activity & capacity
- Stakeholder consultation workshops (Public/Private)
- Legal & Economic analysis (Cost-benefit)
- Regional coordination facilitation
- Policy descision-making workshops for senior officials



EU AML / CFT
GLOBAL FACILITY

Part III: Comprehensive Risk Assessment Framework

Funded by
the European Union

EU AML/CFT GLOBAL FACILITY

Part III: Comprehensive Risk Assessment Framework

Evolution of the Threat Landscape (2024-2025)

The Virtual Assets risk assessment methodology has been updated to reflect the rapid evolution of the threat landscape. The initial focus on Bitcoin has shifted. In 2024 and 2025, stablecoins accounted for over 60% of all illicit transaction volume, surpassing Bitcoin. Criminals favour them for the same reasons legitimate users do: price stability and ease of transfer. This shift requires risk assessments to focus heavily on stablecoin issuers and the "redemption" points where these tokens interact with the banking system.

Methodology for Virtual Asset Risk Assessment

The foundation of any effective virtual asset regulatory regime lies in comprehensive risk assessment that identifies, understands, and evaluates the money laundering and terrorist financing risks associated with virtual asset activities. This assessment must go beyond surface-level analysis to examine the specific characteristics of different virtual asset types, the various business models operating in the ecosystem, and the intersection between virtual assets and traditional financial systems.

The risk assessment process begins with mapping the virtual asset landscape within a jurisdiction. This includes identifying the types of virtual assets in circulation, from established cryptocurrencies like Bitcoin and Ethereum to stablecoins, privacy coins, and tokens associated with decentralised finance protocols. Understanding the technical properties of each asset type is essential, as different technologies present distinct risk profiles. Privacy-enhanced cryptocurrencies with built-in anonymisation features present different challenges than transparent blockchain systems, while stablecoins pegged to fiat currencies may facilitate different illicit finance typologies than volatile cryptocurrencies.

Identifying virtual asset service providers operating within or serving a jurisdiction requires going beyond traditional business registration databases. Many VAs businesses operate entirely online without physical presence, serving customers globally through digital platforms. The assessment must consider not only domestically registered providers but also foreign providers offering services to local residents, peer-to-peer trading platforms, decentralised exchanges accessible to local users, and informal value transfer systems utilising virtual assets.

Data Collection and Analysis Methodologies

Effective risk assessment depends on systematic collection and analysis of both quantitative and qualitative data. Quantitative data sources include suspicious transaction reports filed by financial institutions and virtual asset service providers, law enforcement case statistics involving VAs, customs and border protection data on virtual asset-related financial crimes, and blockchain analytics providing on-chain transaction volumes and patterns. This quantitative foundation must be supplemented with qualitative insights from stakeholder interviews, international cooperation requests, typology studies, academia, and emerging threat assessments.

Analysis methodologies must account for the dynamic nature of VAs risks. Unlike traditional financial products that evolve slowly, virtual asset technologies and business models can emerge and scale rapidly. The risk assessment must therefore be equipped with regular updates to capture new developments. This includes monitoring for new virtual asset types or tokens, emerging business models such as decentralised finance protocols or non-fungible token marketplaces, changes in transaction patterns or volumes, and evolution of illicit finance methodologies.

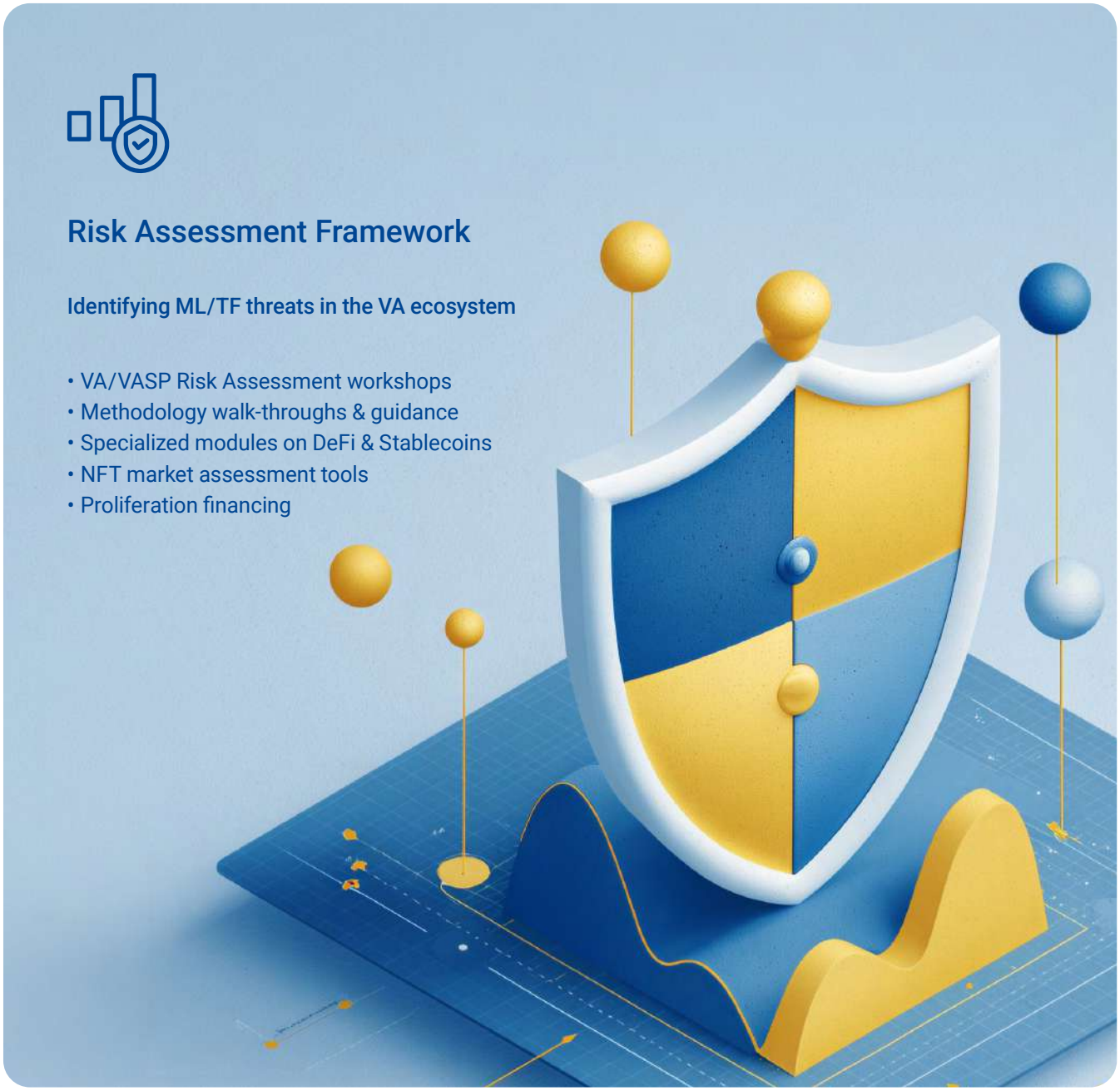
New! Addressing Decentralised Finance and Emerging Technologies

The rise of decentralised finance protocols presents particular challenges for risk assessment. These protocols operate through smart contracts on blockchain networks, enabling financial services

without traditional intermediaries. Assessing risks in DeFi requires understanding not just the technology but also the governance mechanisms, economic incentives, and potential vulnerabilities of these systems.

Non-fungible tokens (NFTs) represent another emerging area requiring specialised risk assessment approaches. While NFTs are often associated with digital art and collectibles, they can also function as vehicles for value transfer or money laundering. Risk assessment must consider the various NFT use cases, from legitimate creative commerce to potential exploitation for financial crime. This includes examining high-value NFT transactions that may represent disguised value transfers, wash trading patterns that artificially inflate NFT values, and the use of NFT marketplaces that lack adequate customer due diligence.

The EU Global Facility is currently aiding several countries regarding the VA Risk Assessment, including providing guidance on conducting VA/VASP Risk Assessment workshops, walk-through on their assessment and others. The enhanced risk assessment framework now includes specialised modules addressing DeFi protocol risks, cross-chain transaction analysis, stablecoin-specific vulnerabilities, NFT market assessment, and proliferation financing indicators.



EU AML/CFT
GLOBAL FACILITY

Part IV: Virtual Asset Service Provider Supervision Framework

Funded by
the European Union

EU AML/CFT GLOBAL FACILITY

Part IV: Virtual Asset Service Provider Supervision Framework

Building Supervisory Capacity and Expertise

Effective supervision of virtual asset service providers requires supervisors to develop deep understanding of both the technology and the business models operating in this space. This represents a significant capacity-building challenge, as traditional financial supervisors may lack the technical expertise to evaluate blockchain-based systems, smart contract risks, or cryptographic security measures.

Supervisory capacity building should begin with foundational training on blockchain technology, cryptographic principles, and VAs ecosystem participants. This technical foundation enables supervisors to engage meaningfully with virtual asset service providers and understand the risks inherent in their operations. Advanced training should cover specific topics relevant to supervision, including transaction monitoring in blockchain environments, smart contract auditing and security assessment, and cross-chain transaction tracking and analysis.

Beyond technical training, supervisors need to understand the business models and economic incentives driving the virtual asset ecosystem. This includes comprehending how centralised exchanges generate revenue and manage risk, understanding the liquidity provision and market-making functions in virtual asset markets, evaluating the custody and security practices of VASPs, and assessing the governance and operational structures of different provider types.

Registration, Licensing, and Ongoing Supervision

The registration or licensing process for virtual asset service providers should be rigorous enough to exclude bad actors while remaining accessible to legitimate businesses. This requires clear eligibility criteria, including fit and proper assessments of beneficial owners and senior management, demonstration of adequate financial resources and operational capacity, comprehensive policies and procedures for AML/CFT compliance, and robust cybersecurity and operational resilience frameworks.

The licensing process should be risk-based, with more stringent requirements for providers offering higher-risk services or serving retail customers. For example, providers offering custody services for customer assets might face additional requirements for segregation of customer assets, insurance or compensation arrangements, and regular third-party audits of security controls. Exchanges facilitating trading in privacy coins or providing services to high-risk jurisdictions might face enhanced due diligence requirements and more frequent supervisory examinations.

Ongoing supervision of licensed virtual asset service providers requires a combination of off-site monitoring and on-site examinations. Off-site monitoring leverages regular reporting from providers, including transaction volumes and patterns, customer complaints and incidents, compliance with prudential requirements, and suspicious activity reports. Advanced supervisory approaches may incorporate blockchain analytics to independently verify provider reporting and identify potential risks or compliance gaps.

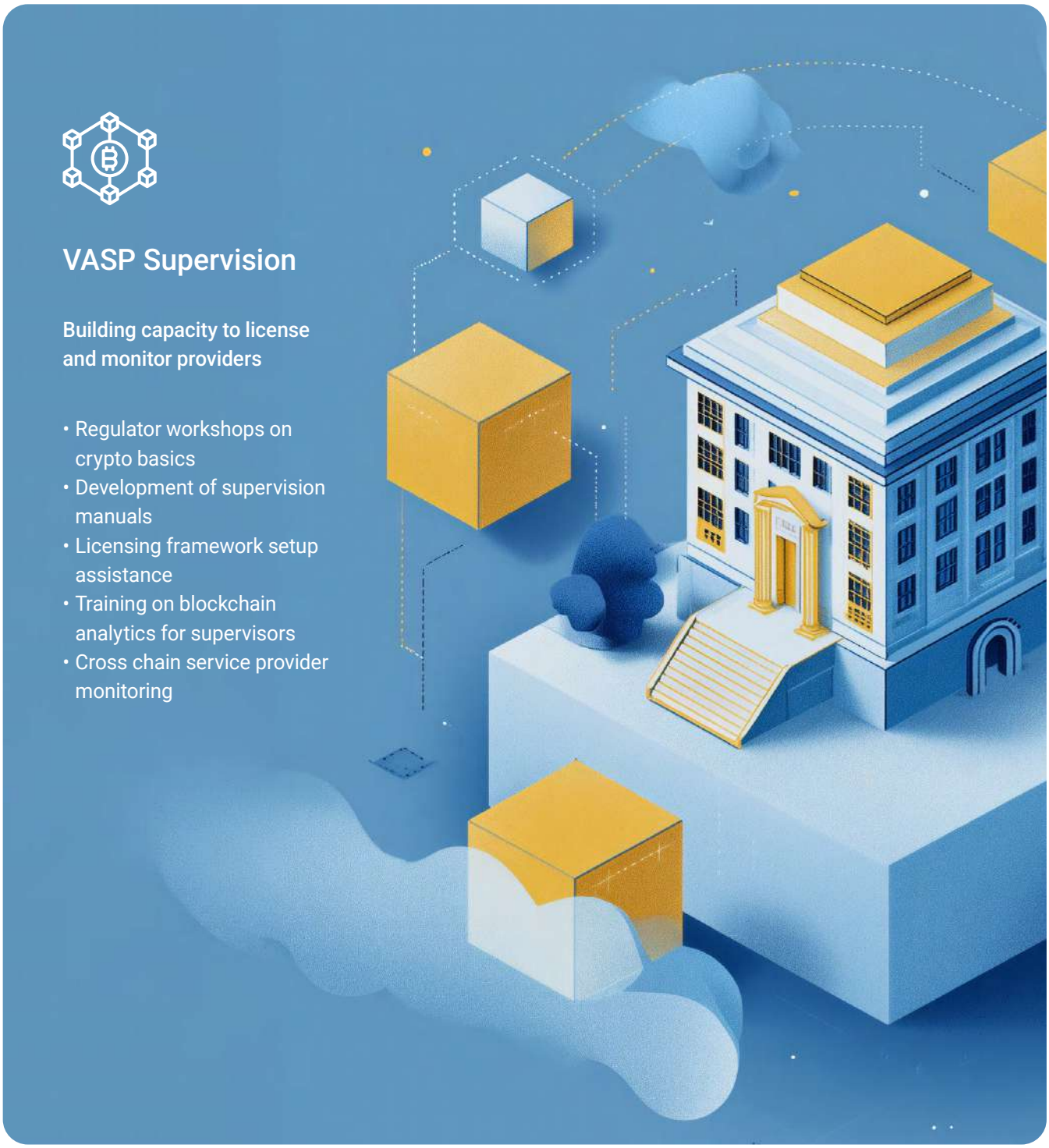
On-site examinations provide deeper insights into provider operations and compliance culture. These examinations should assess the effectiveness of customer due diligence procedures, including customer identification and verification, beneficial ownership determination, and ongoing monitoring. Transaction monitoring systems should be evaluated for their ability to detect suspicious patterns across different virtual asset types and blockchain networks. The examination should also review governance and risk management frameworks, operational resilience and business continuity planning, and compliance with specific regulatory requirements such as the Travel Rule.

Technology-Enhanced Supervision and RegTech Solutions

Technology plays an increasingly important role in enhancing supervisory effectiveness and efficiency. Blockchain analytics tools enable supervisors to

independently monitor virtual asset flows, identify connections between entities, and detect potential illicit activity. These tools can supplement traditional supervisory methods by providing real-time insights into market activity and risk indicators.

EU Global Facility solutions include workshops to regulators to help them understand the basics of cryptocurrencies and how to conduct risk-based approach supervision on VASPs. This assistance can also include setting a framework for supervision on VASPs, including but not limited to indicative supervision manuals. Enhanced training modules now cover DeFi protocol supervision strategies, stablecoin issuer oversight frameworks, cross-chain service provider monitoring techniques, NFT marketplace compliance assessment, and multi-chain transaction surveillance methodologies.



EU AML / CFT
GLOBAL FACILITY

Part V: Investigation & Tracing Capabilities

Funded by
the European Union

Part V: Investigation & Tracing Capabilities

Investigating virtual asset-related crimes requires a fundamental shift in investigative approaches compared to traditional financial crimes. The pseudonymous nature of blockchain transactions, the global reach of virtual asset networks, and the technical complexity of the underlying systems demand new skills, tools, and methodologies for law enforcement agencies.

Blockchain analysis forms the foundation of most virtual asset investigations. This involves examining the public ledger to trace the flow of funds between addresses, identify patterns of behaviour, and ultimately attribute addresses to real-world entities. Effective blockchain analysis requires understanding different blockchain architectures and their implications for traceability, recognising common obfuscation techniques such as mixing services or chain-hopping, and utilising advanced analytics tools that can process vast amounts of blockchain data.

The investigation process typically begins with identifying seed addresses associated with criminal activity. These might come from victim reports, suspicious activity reports from virtual asset service providers, or intelligence from partner agencies. From these seed addresses, investigators can map the flow of funds through the blockchain, identifying intermediate addresses, service providers, and ultimately attempting to identify exit points where VAs are converted to fiat currency or used for purchases.

Attribution remains one of the most challenging aspects of virtual asset investigations. While blockchain analysis can trace the flow of funds between addresses, connecting those addresses to real-world identities requires additional investigative techniques. This might include analysing transaction patterns and timing to identify behavioural signatures, examining blockchain data for inadvertent disclosure of identifying information, coordinating with VASPs to obtain customer information, and utilising traditional investigative techniques such as surveillance or undercover operations.

Cross-Chain Forensics and Advanced Tracing Techniques

The proliferation of cross-chain bridges and multi-chain ecosystems has significantly complicated VAs investigations. Criminals increasingly use cross-chain transfers to obfuscate the trail of illicit funds, requiring investigators to track assets across multiple blockchains with different technical characteristics and data structures.

Cross-chain investigations require comprehensive blockchain coverage and the ability to link transactions across different networks. This involves understanding how different bridge protocols work, including lock-and-mint mechanisms, liquidity pools, and wrapped tokens. Investigators must be able to identify when assets move between chains, track the corresponding transactions on both source and destination chains, and maintain the evidentiary chain despite the technical complexity.

Advanced obfuscation techniques present additional challenges for investigators. Privacy coins with built-in anonymisation features require specialised techniques and tools to trace, if possible at all. Mixing services and tumblers deliberately obfuscate the connection between inputs and outputs, requiring probabilistic analysis and sophisticated clustering algorithms. Decentralised exchanges and automated market makers enable trading without centralised order books, complicating efforts to track fund flows.

Layer 2 solutions and sidechains add another dimension to investigation complexity. These scaling solutions process transactions off the main blockchain, potentially limiting visibility for investigators. Understanding how different Layer 2 solutions work, what data is available for analysis, and how to correlate Layer 2 activity with main chain transactions becomes essential for comprehensive investigations.

Institutional Capacity Building and Training Programmes

Building effective VAs investigation capabilities requires systematic training programmes that address both technical skills and investigative methodologies. Training provided by the EU Global Facility is tailored to different roles within law enforcement and prosecutorial agencies, recognising that not everyone needs the same depth of technical knowledge.

Foundational training for all personnel involved in VAs cases should cover basic blockchain concepts and terminology, understanding of different virtual asset types and their characteristics, overview of the virtual asset ecosystem and its participants, and common typologies and red flags for virtual asset-related crimes. This foundational knowledge enables effective communication and coordination even among personnel who may not directly conduct blockchain analysis.

Specialised training for investigators and analysts should provide hands-on experience with blockchain analysis tools and techniques. This includes practical exercises in tracing transactions across different blockchains, identifying and analysing mixing services and obfuscation techniques, using open-source intelligence to supplement blockchain analysis, and preparing evidence for prosecution while maintaining chain of custody.

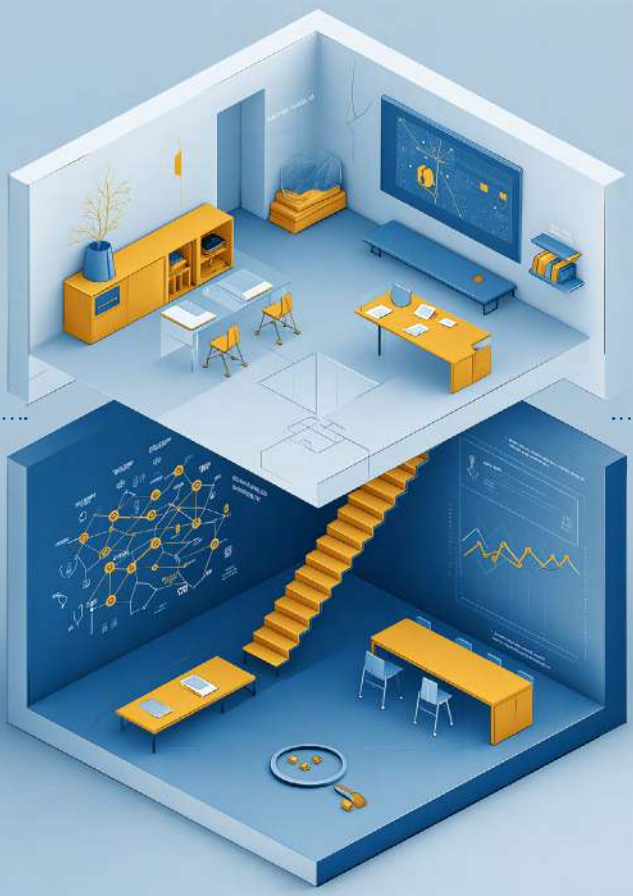
Capacity Building Framework

VIRTUAL ASSET INVESTIGATION & REGULATION

ADVANCED TECHNICAL SKILLS

- Hands-on Analysis
  Practical exercises using blockchain analytics tools.
- Tracing & Attribution
  Following funds across chains and identifying entities.
- Counter-Obfuscation
  Analysing mixers, conjoins, and peel chains.
- Evidence Preparation
  Chain of custody & preparing data for prosecution.

Ensures actionable intelligence and admissible evidence in court.



Level 02

Specialised Training
Target: Investigators & Analysts

PROGRESSION

PROGRESSION

Level 01

Foundational Training
Target: All Personnel

Enables effective communication and coordination across departments

CORE CURRICULUM

- Concepts & Terminology
  Basic blockchain mechanics, wallets, keys, and transfers.
- Asset Types
  Understanding Coins, Tokens, Stablecoins, NFTs, and Defi.
- Ecosystem Overview
  Roles of VASPs, miners, exchanges, and P2P platforms.
- Typologies & Red Flags
  Identifying common partterns of illicit activity.

EU AML/CFT
GLOBAL FACILITY

Investigating & Tracing

Law enforcement tools for the blockchain era

- Foundational training for LEA personnel
- Hands-on blockchain analysis & tracing
- Cross-chain forensics workshops
- Deanonymization & attribution techniques
- Open-source intelligence (OSINT) integration

EU AML / CFT
GLOBAL FACILITY

Part VI: Seizure, Confiscation, and Asset Management

Funded by
the European Union

EU AML/CFT GLOBAL FACILITY

Part VI: Seizure, Confiscation, and Asset Management

Seizing virtual assets presents unique technical and legal challenges compared to traditional asset forfeiture. Unlike physical assets or bank accounts, VAs exist as entries on distributed ledgers, controlled by cryptographic private keys. Effective seizure requires not just legal authority but also technical capability to take control of these private keys and secure the assets against theft or loss.

The seizure process begins with identifying VAs subject to seizure. This might involve tracing illicit funds through blockchain analysis, identifying wallets or addresses controlled by suspects, or discovering private keys during searches of physical or digital devices. Once identified, investigators must determine the most appropriate method for seizure based on the specific circumstances and asset types involved.

For assets held by centralised service providers, seizure might involve serving legal orders on exchanges or custodians to freeze accounts and transfer assets to government-controlled addresses. This approach leverages existing legal frameworks and the compliance obligations of regulated entities. However, it requires rapid action to prevent suspects from moving assets once they become aware of investigation activity.

For self-custody wallets, seizure requires obtaining private keys that control the assets. This might involve forensic analysis of seized devices to extract keys or seed phrases, compelling suspects to provide keys through legal processes, or utilising specialised tools to crack encrypted wallets. Each approach presents technical and legal challenges, requiring careful consideration of proportionality, feasibility, and evidentiary requirements.

Asset Management and Custody Considerations

Once seized, VAs must be securely stored and managed pending final disposition through legal proceedings. This presents significant operational challenges, as government agencies must maintain the security and integrity of seized assets while ensuring appropriate controls and accountability.

Custody solutions for seized VAs range from cold storage using hardware wallets or paper records to institutional custody services provided by specialised firms. Each approach involves trade-offs between security, accessibility, and cost. Cold storage provides maximum security but requires careful key management procedures and may complicate eventual liquidation. Institutional custody services offer professional management and insurance but involve ongoing costs and third-party risk.

The volatile nature of many VAs creates additional management challenges. The value of seized assets can fluctuate dramatically during the often-lengthy legal proceedings, potentially affecting restitution to victims or the value realised upon forfeiture. Some jurisdictions have adopted policies for rapid liquidation of seized VAs to minimise volatility risk, while others maintain assets in kind throughout proceedings.

Management procedures must address not just security but also accountability and transparency. This includes maintaining clear chain of custody documentation, implementing multi-signature or other controls to prevent unauthorised access, regular auditing of seized assets and management procedures, and transparent reporting on the status and disposition of seized assets.

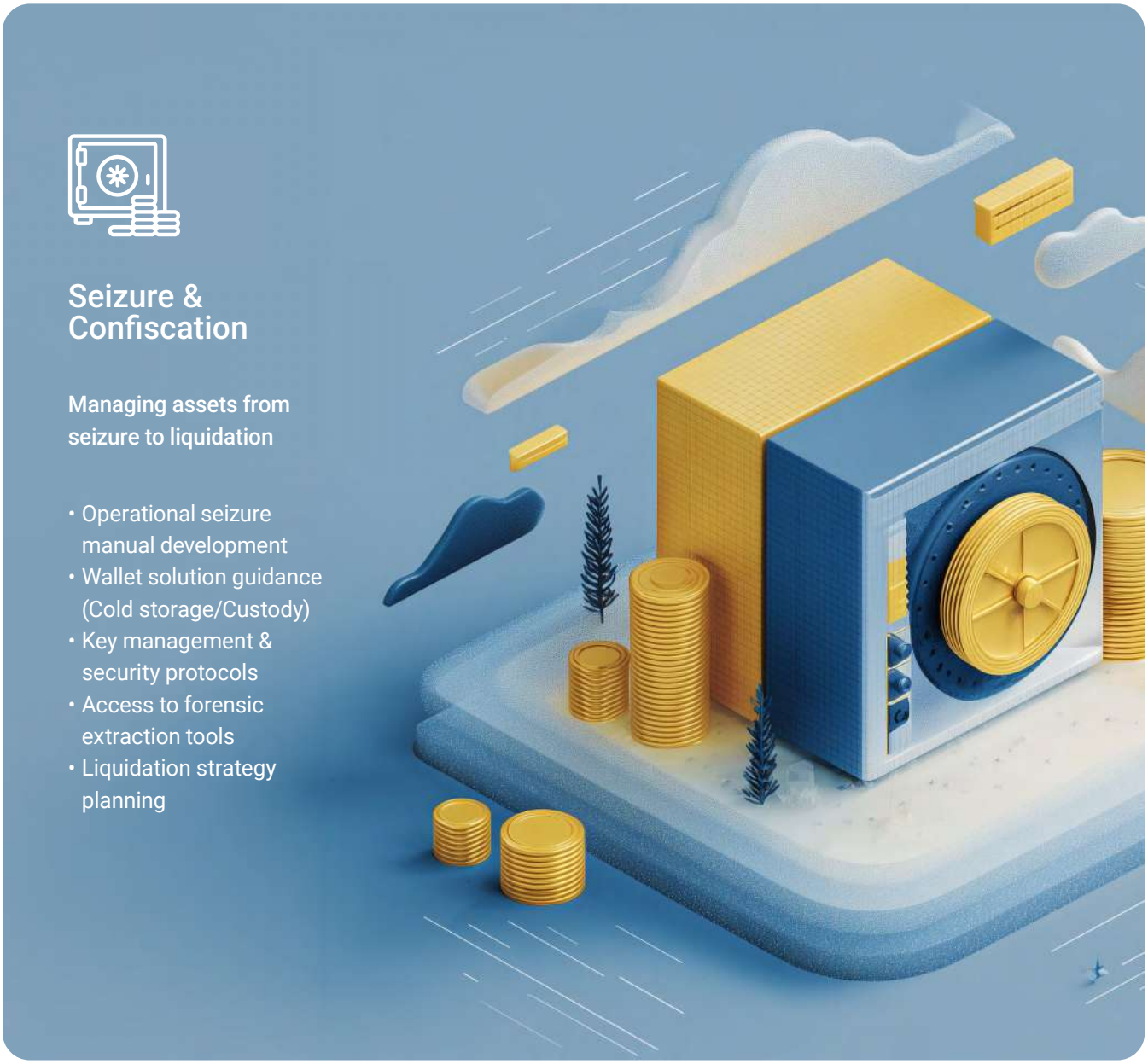
Liquidation Strategies

The eventual liquidation of forfeited virtual assets requires careful planning to maximise value recovery while minimising market impact. Large-scale disposals can significantly affect market prices, particularly for less liquid assets, potentially reducing the value realised and creating broader market instability.

Liquidation strategies might include public auctions that provide transparency and competitive pricing, private sales to institutional investors or market makers, gradual disposal through exchanges to minimise market impact, or retention of certain assets for government use or strategic reserves. The choice of strategy depends on factors including the volume and type of assets, market conditions and liquidity, legal requirements for asset disposal, and policy objectives beyond value maximisation.

Privacy coins and assets associated with illicit activities present particular challenges for liquidation. Many exchanges have delisted privacy coins due to regulatory concerns, limiting liquidity options. Assets directly linked to crimes might be considered tainted, affecting their marketability. Strategies for handling such assets might include working with specialised over-the-counter desks, coordinating with international partners for disposal, or destroying assets in cases where liquidation would be contrary to public policy.

The EU Global Facility provides comprehensive support for countries developing virtual asset seizure and management capabilities through a multi-faceted approach. Our assistance begins with developing detailed yet indicative operational manuals that cover the entire seizure lifecycle - from initial asset identification through forensic extraction of private keys, secure custody, and eventual liquidation. We deliver intensive training programmes tailored to different roles: investigators learn blockchain analysis and digital forensics for extracting keys from devices. The EU Global Facility helps countries choose appropriate wallet solutions based on their seizure volume and security requirements, providing guidance on implementing multi-signature configurations, secure backup procedures, and audit protocols. In collaboration with the private sector, access is facilitated to essential tools including forensic software for key extraction, blockchain analysis platforms for asset tracing, and specialised hardware for secure storage.



EU AML / CFT
GLOBAL FACILITY

Part VII: Addressing Proliferation Financing and Sanctions Evasion

Funded by
the European Union

EU AML / CFT
GLOBAL FACILITY

Part VII: Addressing Proliferation Financing and Sanctions Evasion

Understanding the Proliferation Financing Threat Landscape

The use of virtual assets for proliferation financing and sanctions evasion has emerged as a critical national security concern. State actors and their proxies increasingly exploit the pseudonymous nature of cryptocurrencies to circumvent international sanctions and finance weapons proliferation programmes. This sophisticated threat requires equally sophisticated responses that combine traditional counter-proliferation tools with blockchain-native investigation and enforcement capabilities.

State-sponsored cryptocurrency operations take multiple forms, from large-scale theft of virtual assets through cyber-attacks to cryptocurrency mining operations that generate revenue outside the traditional financial system. The complexity and scale of these operations often exceed typical criminal cryptocurrency use, requiring specialised expertise and international coordination to address effectively.

Understanding proliferation financing through VAs requires mapping the entire value chain from acquisition through laundering to ultimate use. State actors might acquire virtual assets through cyber theft from exchanges or DeFi protocols, ransomware operations targeting critical infrastructure, cryptocurrency mining using state resources or stolen electricity, or front companies and proxies purchasing virtual assets. Once acquired, these assets undergo sophisticated laundering through multiple techniques including chain-hopping across different blockchains, mixing services and privacy coins, over-the-counter brokers in permissive jurisdictions, and complicit or unwitting VASPs.

EU AML/CFT GLOBAL FACILITY

Building Counter-Proliferation Capabilities

Effective counter-proliferation efforts in the VAs space require specialised capabilities that go beyond traditional sanctions enforcement. This includes developing attribution capabilities to identify state-sponsored activity on blockchains, building partnerships with cryptocurrency businesses and blockchain analytics firms, and establishing rapid response mechanisms for addressing identified threats.

Sanctions screening in the virtual asset context presents unique challenges compared to traditional financial sanctions. While traditional screening focuses on names and identifying information, virtual asset screening must also address blockchain addresses and transaction patterns. This requires maintaining comprehensive databases of sanctioned addresses, implementing real-time screening of blockchain transactions, developing risk indicators for potential sanctions evasion, and coordinating with international partners on address attribution and designation.

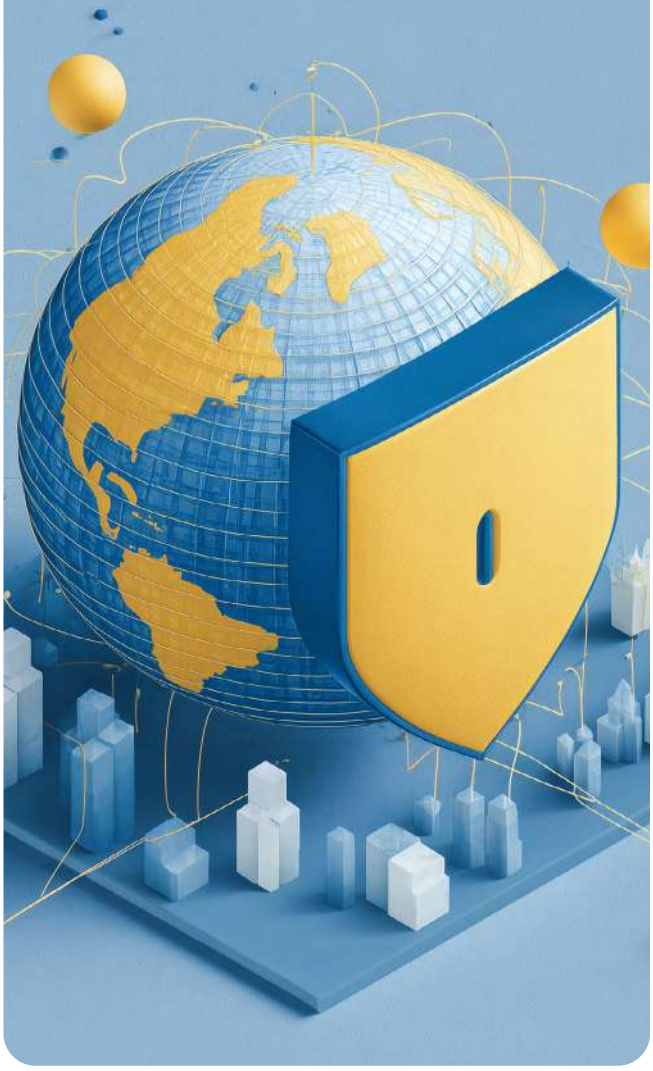
The EU Global Facility provides comprehensive support for countries conducting virtual asset risk assessments specifically focused on proliferation financing threats, helping them understand and document how sanctioned actors like Democratic People's Republic of Korea (DPRK) and Iran exploit cryptocurrencies to evade international sanctions. Our risk assessment framework examines the complete threat landscape, analysing DPRK's sophisticated cryptocurrency theft operations that have stolen billions from exchanges and DeFi protocols, their use of IT workers operating under false identities to earn cryptocurrency, and their deployment of ransomware against critical infrastructure for revenue generation.

The EU Global Facility delivers specialised training programmes that deep-dive into the specific modus operandi of state-sponsored cryptocurrency operations, using real case studies from DPRK's Lazarus Group heists, Iran's bitcoin mining revenue generation, and sanctions evasion networks operating across multiple jurisdictions. The training includes hands-on exercises using sanitised data from actual investigations, teaching participants to trace stolen funds through multiple hops and mixers, identify convergence points where state actors cash out, and recognise behavioural patterns that distinguish state-sponsored from criminal activity.

Proliferation financing

Countering state-sponsored sanctions evasion.

- DPRK/Iran specific threat analysis
- Advanced attribution training
- Sanctions evasion pattern recognition
- Tracing stolen funds through mixers
- Counter proliferation risk assessments



EU AML / CFT
GLOBAL FACILITY

Part VIII: Implementation Roadmap and Capacity Building

Funded by
the European Union

EU AML/CFT
GLOBAL FACILITY

Part VIII: Implementation Roadmap and Capacity Building

Implementing a comprehensive virtual asset framework requires a carefully phased approach that builds capabilities incrementally while maintaining effectiveness at each stage. Countries should begin with foundational elements before moving to more advanced capabilities, ensuring that each phase builds on solid foundations rather than attempting to implement everything simultaneously.

The initial phase focuses on establishing legal and regulatory foundations. This includes developing or updating legislation to address VAs and VASPs, establishing regulatory authority and coordination mechanisms among relevant agencies, and conducting initial risk assessment to understand the VAs landscape. This phase also involves basic capacity building to ensure that key personnel understand virtual asset technology and risks.

The second phase implements core regulatory and supervisory functions. This includes establishing registration or licensing requirements for VASPs, implementing basic AML/CFT requirements such as customer due diligence and suspicious activity reporting, and developing supervisory procedures for monitoring compliance. Law enforcement agencies begin developing investigation capabilities, starting with basic blockchain analysis and coordination with regulated entities.

Advanced implementation phases add sophisticated capabilities such as cross-chain investigation and complex forensics, supervision of DeFi interactions and emerging technologies, international cooperation and cross-border enforcement, and specialised units for high-priority areas such as proliferation financing. These advanced capabilities require significant investment in technology, training, and institutional development.

Phased Implementation Strategy

A STRUCTURED ROADMAP FOR BUILDING COMPREHENSIVE VIRTUAL ASSET CAPABILITIES, MOVING FROM FOUNDATIONAL LEGISLATION TO ADVANCED ENFORCEMENT.

PHASE 01

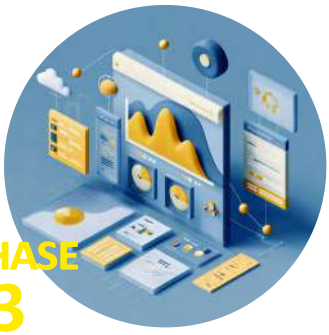
Foundations & Legal Framework

- **Legislation**: Update laws to define VAs and VASPS.
- **Authority Setup**: Designate regulatory bodies and coordination mechanisms.
- **Risk Assessment**: Analyse the national VA landscape and threats
- **Basic Capacity**: Train key personnel on technology basics and risks.

PHASE 02

Core Regulatory & Supervisory Functions

- **Licencing Regime**: Registration requirements for VASPs to operate legally.
- **AML/CFT Controls**: Mandate KYC, customer due diligence, and suspicious reporting.
- **Supervision**: Monitor compliance and conduct examinations.
- **Basic Investigation**: Start blockchain tracing and regulated entity coordination.



PHASE 03

Advanced Capabilities & Enforcement

- **Complex Forensics**: Cross-chain investigations and analysis of obfuscation techniques.
- **Global Enforcement**: International cooperation and cross-border asset recovery.
- **DeFi & Emerging Tech**: Supervision of decentralised protocols and smart contracts.
- **Specialised Units**: Dedicated teams for high-priority threats (e.g. proliferation financing).

Through implementation, countries should maintain flexibility to adapt their approach based on evolving risks and lessons learned. Regular review and updating of the framework ensure continued effectiveness as the virtual asset ecosystem evolves. This includes monitoring international developments and best practices, assessing the effectiveness of implemented measures, and adjusting approaches based on experience and changing circumstances.

Conclusion

Towards a comprehensive virtual asset framework

The VAs ecosystem continues to evolve at a rapid pace, presenting both opportunities for financial innovation and challenges for regulatory oversight. The comprehensive framework presented in this document provides countries with the tools and approaches needed to address these challenges while supporting responsible innovation.

Success in regulating virtual assets requires recognising that this is not merely a technical or legal challenge but a fundamental shift in how value moves through the global financial system. Countries must develop new capabilities, adopt new approaches, and maintain flexibility to adapt as technology evolves. The framework presented here provides a roadmap for this journey, but each country must chart its own course based on its specific circumstances, risks, and objectives.

The EU Global Facility stands ready to support countries in implementing comprehensive VAs frameworks that protect against illicit finance while enabling legitimate use of these transformative technologies. Through technical assistance, capacity building, and knowledge sharing, we can work together towards a safer world that harnesses the benefits of virtual assets while mitigating their risks.

THE EUROPEAN UNION'S GLOBAL FACILITY ON

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

www.global-amlcft.eu

EU Global Facility on AML/CFT

Funded by the European Union

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the EU AML/CFT Global Facility and do not necessarily reflect the views of the European Union.