www.rusi.org

RUSI

# Institutional Virtual Asset Service Providers and Virtual Assets Risk Assessment Guide

Noémi També and
Allison Owen

August 2023

192 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.



Published in 2023 by the Royal United Services Institute for Defence and Security Studies.



Published August 2023

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

# Contents

# Acknowledgements

This guide was completed as part of the Centre for Financial Crime and Security Studies' ongoing work in relation to sanctions implementation and the vulnerabilities of the financial system to the facilitation of sanctions circumvention. It was funded through a grant from the US State Department's Office of Cooperative Threat Reduction.

The authors would like to thank James Gillespie and Rodrigo Peiteado for their review and helpful comments on an earlier version of this document. A special thanks is also due to Yannick Cherel for offering his insight as part of the research for developing this guide and to all those who have generously offered their time to be interviewed. The authors are also grateful to the RUSI Publications team for their work on this guide.

# Acronyms

| | |
|---|---|
| **AFC** | anti-financial crime |
| **AML** | anti-money laundering |
| **CEX** | centralised exchange |
| **CDD** | customer due diligence |
| **CPF** | counter proliferation finance |
| **CTF** | counter terrorist finance |
| **DeFi** | decentralised finance |
| **DEX** | decentralised exchange |
| **EDD** | enhanced due diligence |
| **FATF** | Financial Action Task Force |
| **FCP** | financial crime prevention |
| **FIU** | Financial Intelligence Unit |
| **ICO** | initial coin offering |
| **ID&V** | identification and verification |
| **IP** | internet protocol |
| **KYC** | 'know your customer' |
| **ML** | money laundering |
| **MSB** | money services business |
| **NFT** | non-fungible token |
| **OTC** | over the counter trader |
| **PEP** | politically exposed person |
| **PF** | proliferation financing |
| **P2P** | peer-to-peer |
| **RA** | risk assessment |
| **RBA** | risk-based approach |
| **SAR** | suspicious activity report |
| **SDD** | simplified due diligence |
| **TF** | terrorist financing |
| **VA** | virtual asset |
| **VASP** | virtual asset service provider |
| **VPN** | virtual private network |

# Executive Summary

The process of identifying crypto-related financial crime red flags within the private sector lacks uniformity. Two centralised cryptocurrency exchanges with similar risk appetites, services and transaction volumes can have different criteria to determine what qualifies as a high-risk transaction. To compound this problem, the institutional risk assessments that crypto businesses create are often proprietary. Publicly available guides on how to successfully assess risks within this fast-paced industry are non-existent. The private sector, including virtual asset service providers (VASPs) and financial institutions (FIs), needs such a guide to assess risk, identify suspicious activity and flag the information to the relevant authorities.

This guide is designed to provide a standardised approach to assessing financial crime risk within the cryptocurrency industry. It documents observed and emerging risks to allow institutions to identify high-risk activities and determine strategies to tackle such risks. Furthermore, the virtual assets risk assessment framework provided will help institutions better understand and define their risk appetite while being aligned to virtual asset laws and regulations.

The guide documents how VASPs and FIs should understand the crypto-related financial crime risks they face through customers, the tokens and services they offer, jurisdictions in which and with which they operate, transactions, delivery channels, fraud, and cyber threats. It further explains how these institutions could assess the inherent risk of these categories by considering the likelihood of the risk materialising based on their business model, alongside any potential impact it would have.

After the inherent risk is evaluated, the institution needs to assess residual financial crime risks. This is achieved by assessing the effectiveness of existing controls in place to tackle inherent risks. Once the institution completes its virtual assets risk assessment, it can then measure its residual risks and decide whether to accept or further mitigate them.

# Introduction

With global compliance and regulation lacking in many jurisdictions, virtual asset service providers (VASPs) can present an easy target for criminals engaging in money laundering (ML), terrorist financing (TF) and proliferation financing (PF).

This guide aims to:

- Support VASPs in identifying and assessing their ML, TF and PF risks.
- Document strategies to tackle ML, TF and PF risks as per Financial Action Task Force (FATF) Recommendations 1, 2, 3, 5, 6, 7, 10, 11, 12, 15 and 16.[1]
- Document best-practice compliance when dealing with ML, TF and PF risks.

It provides practical support and guidance to:

- Fully regulated VASPs, as well as VASPs located in immature markets and/or operating within jurisdictions with immature regulatory frameworks.
- Financial institutions (FIs) that wish to add crypto assets, products and services to their offering.
- FIs that wish to provide banking services and products to VASPs.

Chapter I discusses four factors that make some VASPs more vulnerable to ML, TF and PF risks. Chapter II documents case studies of VASPs' ML, TF and PF abuse, and suggests targeted risk mitigation strategies that they should consider implementing to tackle such threats. Chapter III provides best practices for a compliance framework, including processes and controls, to mitigate financial crime risks. It also documents the risk assessment framework informed by the authors' research.

This document should be read in conjunction with the ML, TF and PF national risk assessments available in, or relevant to, an institution's and the FATF guidance on virtual assets risk assessments.[2]

1. FATF, 'FATF 40 Recommendations', <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>, accessed 12 February 2023.
2. FATF, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', 28 October 2021, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>, accessed 28 June 2023.

# Methodology

The research for this guide is informed by interviews with relevant stakeholders in the virtual asset service providers industry, including blockchain analytics and law enforcement agencies (LEAs). Ten financial crime risk practitioners and experts were selected based on their expertise and experience across the crypto industry. They were interviewed between October 2022 and April 2023. The qualitative data collated from interviews was validated through discussions with consultants and a review of relevant policy literature, reports from supervisors across several jurisdictions and grey literature.[3]

This guide does not explore blockchain analytics tools and solutions.

# Definitions and Scope

This section defines the way in which the terms 'virtual asset' (VA) and 'VASP' are used in this guide. It also documents the rationale for including specific crypto business models and assets within the risk assessment scope.

According to the FATF, the international standard-setter for countering ML, TF and PF, a VA is a 'digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes'.[4] For the purpose of this guide, the authors have adopted this definition.

The authors include non-fungible tokens (NFTs)[5] within the scope of the framework, although their diversity (such as those that represent collectibles, physical property or use tokens as collateral) challenges VA classification. In addition, the FATF allows jurisdictions to decide whether NFTs fall under the definition of a VA, despite stating that NFTs 'are unique and used in practice as collectibles rather than as payment or investment instruments'.[6]

3. The grey literature includes FATF guidance documents, national risk assessments for virtual assets, and reports from the HM Treasury, US Treasury, the Financial Stability Board, blockchain analytics companies and regulators' enforcement actions.
4. Virtual assets do not include digital representations of fiat currencies backed by a central bank (also known as central bank digital currencies), securities and other financial assets that are already covered by FATF Recommendations. See FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', updated February 2023, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>, accessed 29 March 2023.
5. Unique tokens that represent a digital or physical asset that are purchased with cryptocurrency.
6. FATF, 'Targeted Update on Implementation of FATF's Standards on VAs and VASPs', 30 June 2022, p. 20, <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html>, accessed 30 March 2023.

Similarly, with the FATF noting that stablecoins[7] 'will either be considered a virtual asset or a traditional financial asset depending on its exact nature',[8] this guide includes these within the scope of the framework for the sake of completeness.

The reader should note that there are approximately 23,000 different cryptocurrencies as of April 2023.[9] Table 7 in the Annex lists and defines the types of tokens that were discussed during interviews and identified through open source research. Due to the industry's fast pace, Table 7 is not exhaustive.

The FATF defines VASPs as any natural or legal person or business that carries out the following activities on behalf of another natural or legal person:

- Exchange between cryptocurrency and fiat currency.
- Exchange between one or more forms of cryptocurrency.
- Transfer of cryptocurrency.
- Holding custody of cryptocurrency or administration of instruments that enable custody.
- Participation in financial services related to an issuer's offer or sale of cryptocurrency.[10]

The authors adopt this definition and document businesses that can fall under this category in Table 8 of the Annex.

7. Tokens that are pegged 1:1 to a valuable item, such as fiat currency, cryptocurrency or natural resources.
8. FATF, 'FATF Report to G20 on So-Called Stablecoins', 7 July 2020, p. 2, <https://www.fatf-gafi.org/en/publications/Virtualassets/Report-g20-so-called-stablecoins-june-2020.html>, accessed 30 March 2023.
9. CoinMarketCap, 'Today's Cryptocurrency Prices by Market Cap', 3 April 2023, <https://coinmarketcap.com/>, accessed 3 April 2023.
10. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', amended February 2023, p. 135, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>, accessed 13 July 2023.

# I. Financial Crime Risks and Elevated Risk Factors

Informed by the authors' interviews, this chapter documents criteria that make some VASPs more vulnerable to ML, TF and PF risks.

Interviewees indicated that there are four risk factors that increase exposure to ML, TF and PF risks. These are:

- Uneven regulatory oversight.
- End user opacity.
- Capacity to obfuscate the money trail.
- Ability to convert fiat currency into cryptocurrency and vice versa.

The factors are discussed in turn below.

## Uneven Regulatory Oversight

The lack of homogeneous regulation and standards across the industry is a source of concern.[11] Uneven implementation of crypto asset regulations enables criminals to carry out regulatory arbitrage. For instance, they may seek to launder illicitly acquired funds in VASPs located in jurisdictions with weak anti-financial-crime (AFC) frameworks while avoiding countries with more robust AFC systems, processes and controls. Interviewees indicated that, when onboarding individuals or institutional customers, the country of residency, incorporation or place of business is a risk indicator that influences the risk score applied to their customers.[12]

As illustrated below, another element identified as a source of concern is VASPs escaping liability because they are not physically based in the countries where their companies are incorporated. Under such circumstances, these VASPs can

11. Authors' interview with expert 10, 10 April 2023.
12. Authors' interviews with expert 1, 21 October 2022; expert 3, 24 February 2023; expert 5, 14 March 2023; expert 6, 21 March 2023; expert 7, 23 March 2023; expert 9, 27 March 2023; expert 10, 10 April 2023. It should be noted that this is aligned to the FATF's updated guidance on a risk-based approach to VAs and VASPs, which states that 'countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, especially for VASPs, and for which VASPs and other obliged entities should give special attention to business relationships and transactions'. See FATF, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', p. 50.

limit their accountability towards jurisdictions' LEAs and/or financial intelligence units (FIUs).[13] This disrupts AFC efforts and challenges investigative initiatives.[14] A complaint in March 2023 from the Commodities Futures Trading Commission (CFTC) against a high-profile centralised exchange (CEX) echoes this point, explaining that while the CEX 'has maintained offices in numerous locations, including Singapore, Malta, Dubai, and Tokyo at various times during the relevant period, [it] intentionally does not disclose the location of its executive offices. Instead, [the company's CEO] has stated that [the CEX]'s headquarters is wherever he is located at any point in time, reflecting a deliberate approach to attempt to avoid regulation'.[15]

An additional element that was raised is the cross-border nature of cryptocurrency and VASPs. This creates further difficulties for LEAs that need to work with jurisdictions with less mature AFC frameworks or limited resources. Those jurisdictions may not respond in a timely manner and/or adequately to requests for information[16] concerning VASPs incorporated in such countries.[17]

# End-User Opacity

Research also identified the opacity of end users as a risk factor. VASPs that do not implement robust 'know your customer' (KYC) and customer due diligence (CDD) policies and do not apply the travel rule[18] have little to no visibility of who their customers are. For instance, both the March 2023 CFTC complaint and a January 2023 New York Department of Financial Services consent order document observed AFC framework weaknesses within two separate CEXs. Indeed, the latter document states that 'the Department's Examination found significant deficiencies across [the CEX] compliance program, including its Know Your

13. Authors' interview with expert 7, 23 March 2023.
14. It should be noted that the FATF's Interpretive Note to Recommendation 15 aims to prevent such instances, stating: 'At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created'. See FATF, 'FATF Recommendations, 2012–2022', p. 76, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html#:~:text=As%20amended%20February%202023.,of%20weapons%20of%20mass%20destruction>, accessed 27 June 2023.
15. *CTFC v. Changpeng Zhao, Binance Holdings Limited, Binance Holdings (IE) Limited, Binance (Services) Holdings Limited, and Samuel Lim,* US District Court for the Northern District of Illinois, 27 March 2023, p. 3, <https://www.cftc.gov/media/8351/%20enfbinancecomplaint032723/download>, accessed 27 June 2023.
16. 'The FIU exchanges information with other local agencies based on the legislation and regulations authorising such exchanges. In some countries, FIUs have used memoranda of understanding or similar documents to make more detailed arrangements for exchanging information authorised by law with other agencies with which they exchange information on a regular basis'. See IMF, 'FIUs: An Overview', 2004, p. 64, <https://www.imf.org/external/pubs/ft/fiu/fiu.pdf>, accessed 30 April 2023.
17. Authors' interview with expert 9, 27 March 2023.
18. According to FATF, VASPs must collect information on the originator and beneficiary of all transactions authorised. This requirement is known as the 'travel rule'.

Customer/Customer Due Diligence ("KYC/CDD") procedures, its Transaction Monitoring System ("TMS"), and its OFAC [Office of Foreign Assets Control] screening program. The Examination also found that [the CEX] failed to conduct adequate annual Anti-Money Laundering ("AML") risk assessments'.[19]

In sum, CEXs that let individuals trade crypto assets without adequate compliance measures in place are exposed to higher financial crime risks, as they may inadvertently provide products and services to criminals and sanctioned actors, thus facilitating the laundering of illicit gains.[20]

Interviews also indicate that although some decentralised finance (DeFi) services implement robust KYC and CDD, such platforms are vulnerable to financial crime risk.[21] DeFi enables users to perform cryptocurrency payments and services with no intermediaries or centralised authority such as a bank.[22] DeFi services do not routinely collate CDD, KYC or source of wealth information, which is unsurprising since DeFi's raison d'être is disintermediation and decentralised banking. For example, decentralised exchanges (DEXs) do not require an intermediary to manage funds. Transactions are instead executed through smart contracts,[23] allowing users to trade VAs without verifying their identity. The growing awareness of the financial crime risks associated with DeFi services are documented in the US Treasury Department's 2023 report, 'Illicit Finance Risk Assessment of Decentralized Finance',[24] and the FATF's 2020 'Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers'.[25] As the FATF notes, there continue 'to be persons and centralised aspects that may be subject to AML/CFT obligations' for DeFi-branded projects.[26] Accordingly, this may be indicative of reduced exposure to ML, TF or PF when considering financial crime risks associated

19. New York State Department of Financial Services, 'In the Matter of Coinbase, Inc., Respondent', Consent Order, 2023, p. 4, <https://www.dfs.ny.gov/system/files/documents/2023/01/ea20230104_coinbase.pdf>, accessed 1 February 2023.
20. Authors' interviews with expert 1, 21 October 2022; expert 3, 24 February 2023; expert 5, 14 March 2023; expert 10, 10 April 2023.
21. Authors' interviews with expert 4, 1 March 2023; expert 9, 27 March 2023; expert 10, 10 April 2023.
22. DeFi offers products and services similar to mainstream financial services, such as loans, staking, trading or mixing services. DeFi makes use of 'smart contracts' and therefore does not rely on a central entity responsible for asset custody, transactions flows or payments. Instead of a central body, smart contracts specify and guarantee the terms and conditions for the execution of operations.
23. 'Smart contracts are contracts that are coded and stored on the blockchain. They automate agreements between the creator and recipient, making them immutable and irreversible. Their primary purpose is to automate the execution of an agreement without intermediaries, ensuring that all parties can confirm the conclusion instantly'. See CoinTelegraph, 'What is a Smart Contract and How Does it Work?', <https://cointelegraph.com/learn/what-are-smart-contracts-a-beginners-guide-to-automated-agreements>, accessed 17 April 2023.
24. US Department of the Treasury, 'Illicit Finance Risk Assessment of Decentralized Finance', April 2023, <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>, accessed 17 April 2023.
25. FATF, 'Targeted Update on Implementation of FATF's Standards on VAs and VASPs'.
26. *Ibid.*

with DeFi projects and an area for which institutions wishing to conduct business with DeFi need to complete a risk assessment. Chapter III details how to conduct one.

## Capacity to Obfuscate the Money Trail

Another identified risk factor is the ability of certain VASPs to obfuscate money trails. Such VASPs are more likely to be exploited because they may facilitate the layering stages of ML and might support terrorist and proliferation financiers in moving and disguising funds.[27]

A VASP can leverage the services offered by another VASP on behalf of its own clients. For example, over the counter traders (OTCs)[28] who facilitate decentralised high-value trading may operate via a high-volume CEX. Typically, the OTC will declare this activity to the CEX in question during the onboarding process[29] and provide evidence that it has robust systems and controls in place to mitigate financial crime risks. Similarly, the onboarding VASP should apply additional controls to mitigate risks associated with providing services to OTCs. However, an unscrupulous OTC may fail to disclose its activities and operate as an OTC without the onboarding VASP's knowledge.

Similarly, nested exchanges, whereby a business uses the liquidity of a larger exchange to provide trading and investment services to clients, also enable such obfuscation.[30] The nested exchange may or may not flag this activity with the onboarding VASP. Box 1 illustrates the case of nested exchange services that facilitated transactions for ransomware actors.

27. The three stages of ML are placement, layering and integration. The three stages of TF are fundraising, moving the funds and using the funds. Finally, the three stages of PF are fundraising, disguising and placing funds into the financial system, and using the funds to procure materials and technology needed for WMD programmes. For more information on the three stages of PF, see Noémi També, 'Institutional Proliferation Finance Risk Assessment Guide', RUSI, 8 June 2023.
28. CEXs are platforms that act as an intermediary between buyers and sellers of cryptocurrencies. OTC trading provides a market for dealers and brokers, enabling users to interact directly with one another and transact large sums and volumes of cryptocurrency.
29. When a customer signs up to an FI's product or services, they will be set up on the institution's platform and submitted to an onboarding process where the customer's information is recorded.
30. Authors' interviews with expert 2, 14 February 2023.

**Box 1: Ransomware Actors and Nested Exchanges**

In November 2021, the US Department of the Treasury announced the designation of Chatex, a VA exchange that facilitated transactions for ransomware actors. Chatex had direct ties to Suex, which the US had sanctioned two months prior. According to the announcement, Chatex used 'Suex's function as a nested exchange to conduct transactions'. Suex acted as a 'nested' exchange and took advantage of services at other VASPs to allow customers to transact.

Sources: US Department of the Treasury, 'Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange', 8 November 2021, <https://home.treasury.gov/news/press-releases/jy0471>, accessed 3 April 2023; TRM Labs, 'Behind Suex.io: The First Sanctioned Cryptocurrency Exchange', 21 September 2021, <https://www.trmlabs.com/post/behind-suex-io-the-first-sanctioned-cryptocurrency-exchange>, accessed 3 April 2023.

The risk of unknowingly providing services and products to unidentified nested exchanges can be mitigated during customer onboarding and transaction monitoring. Chapter III discusses verification mechanisms to detect this activity.

Along with nested exchanges, experts identified cross-chain bridge exploits,[31] coin-swapping,[32] chain-hopping[33] and mixers[34] as elevated risk factors.[35] Advances in the underlying technology for these applications, as well as enhanced cyber security measures, may restrict cross-chain bridge and DEX exploitation in the medium term, but VASPs should be alert to the risks they pose nonetheless. In contrast, the use of mixers will continue to be a challenge.[36] This will require quicker de-mixing capabilities for investigative purposes and enhanced training on this process for law enforcement. Due to the anonymity-enhancing characteristics of these applications, incoming transactions linked to these services may represent a higher risk. Although legitimate reasons for these applications exist, evidence suggests that sanctioned and criminal actors often abuse them to launder funds.

31. Cross-chain exploits enable users to exchange VAs from one blockchain to another. For more information, see Elliptic, 'The State of Cross-Chain Crime', 2022, <https://www.elliptic.co/resources/state-of-cross-chain-crime-report>, accessed 17 April 2023; US Department of the Treasury, 'Illicit Finance Risk Assessment of Decentralised Finance'.
32. Crypto swapping involves directly trading one cryptocurrency for another.
33. The process of converting between cryptocurrencies, sometimes in a brief duration of time, to disrupt investigations.
34. Users may use crypto mixers to keep their transactions private, by mixing their cryptocurrency funds with vast sums of other crypto funds. Crypto mixing services may be centralised or decentralised. Mixers are used to anonymise funds between services and do not perform CDD/KYC checks.
35. Any services with a weak KYC, CDD, AML, CTF and CPF framework will be leveraged to obfuscate users and the money trail.
36. Authors' interview with expert 8, 24 March 2023.

# Ability to Convert Between Fiat and Crypto Assets and Vice Versa

Finally, interviewees explained that CEXs are attractive for ML because they enable the exchange of fiat money for crypto assets (on ramps) and the exchange of crypto assets for fiat money (off ramps). Illicitly acquired crypto assets most likely will be exchanged into fiat money and alternatively, illicitly acquired fiat into crypto to enable the placement, layering and integration stages of ML,[37] as well as the moving and use of funds in TF and PF. Indeed, a 2023 report by a blockchain analytics firm notes that 'this is the most important part of the money laundering process, as the funds can no longer be traced via blockchain analysis once they hit a [fiat off ramp] service'. This risk is enhanced if the off ramp, or conversion from crypto assets to fiat currency, results in the customer requesting a wire transfer to a bank in a high-risk jurisdiction or an account that is not in the customer's name.

Another VASP type that enables fiat on ramps and off ramps, thus representing a higher financial crime risk, is a crypto ATM.[38] Crypto ATMs enable users to buy and sell crypto in exchange for fiat currency, facilitating fiat on ramps and off ramps, sometimes with no KYC or CDD performed. For instance, the Financial Market Supervisory Authority (FINMA), the Swiss regulator, indicated in its 2021 annual report that drug dealers are using crypto ATMs for payment.[39] Similarly, a 2022 typology report published by a crypto analytics company documents the vulnerabilities of crypto ATMs to illicit transfers, mule activities and scams.[40] As an indication of the elevated risk factor that crypto ATMs represent, some jurisdictions such as the UK have no official crypto ATMs registered with local regulators, due to ineffective AFC controls.[41] It should be noted, however, that neither report provides data relating to transaction volumes or frequency. In addition, further open source research did not provide the authors with additional data on the scale of the issue. The private sector should conduct additional research to assess and measure the scale of illicit crypto ATM use to ensure that regulatory supervision and AFC efforts remain risk based.

37. Authors' interviews with expert 6, 21 March 2023; expert 8, 24 March 2023; and expert 10, 10 April 2023.
38. Authors' interview with expert 6, 21 March 2023.
39. FINMA, 'Annual Report', 2021, <https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20220405-finma_jahresbericht_2021.pdf?sc_lang=en&hash=39D0EED3823CAE735B128E31DE0FDAD1>, accessed 1 May 2023.
40. Elliptic, 'Preventing Financial Crime in Cryptoassets: Typologies Report 2022', 2022, p. 42, <https://www.elliptic.co/resources/typologies-report-2022>, accessed 17 April 2023.
41. Kalyeena Makortoff, 'Watchdog and West Yorkshire Police Raid Crypto ATM Operators in UK First', *The Guardian*, 14 February 2023.

With this understanding of the four risk factors that make some VASPs more vulnerable to financial crime than others in mind, and to bring these risk concepts to life, Chapter II will document five case studies where VASPs are abused for the purpose of financial crime. It will also discuss controls that should be implemented to tackle weaknesses and mitigate financial crime risks.

# II. Risk Mitigation Strategies

This chapter provides an analysis of risk mitigation strategies in response to ML, TF and PF examples within the crypto industry. Specific measures to address vulnerabilities are documented following each case study. It is critical to note that this chapter does not present an exhaustive list of financial crime mitigation strategies.

## Money Laundering

The cryptocurrency industry is abused for ML, often because criminals think that cryptocurrency transactions are difficult to track. However, open source platforms now attribute cryptocurrency addresses to criminal activity, making the tracing process easier, even if an individual does not have access to blockchain analytics tools. But criminals have deployed advanced ML techniques to keep up with these capabilities, as shown in the following case study.

**Box 2: Bitfinex Hack**

In 2022, two individuals, Ilya Lichtenstein and Heather Morgan, were arrested on a charge of laundering stolen cryptocurrency from a 2016 hack of Bitfinex, a cryptocurrency exchange. More than 2,000 unauthorised transactions occurred on account of the hack, sending stolen Bitcoin to a wallet that Lichtenstein controlled. Lichtenstein and Morgan laundered approximately 25,000 of the stolen tokens. The criminals used fake identification to set up online accounts and used applications that allow for automated transactions to take place within a short span of time. In addition, they used crypto exchanges and darknet markets, converting between different cryptocurrencies (including privacy coins) and using US business accounts to legitimise banking activity.

At one of the exchanges, accounts were identified through the following information:

- Email addresses were hosted by the same India-based provider.
- The same IP addresses accessed accounts.

- Accounts were created around the time of the hack.
- Accounts engaged in the same trading patterns (chain-hopping, anonymity-enhancing tokens).
- When asked for KYC information, account activity stopped.

In a separate exchange, Morgan sent the incorporation documents of a company known as SalesFolk, with herself as the sole owner. A shell company claiming to operate in Hong Kong sent virtual currency to SalesFolk, which Morgan claimed was for advertising services. Funds from the crypto exchange were converted to fiat currency and sent to accounts held by Lichtenstein and Morgan at a US-based financial institution.

Sources: US Department of Justice, 'Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency', 8 February 2022, <https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency>; US Department of Justice, 'Case 1:22-mj-00022-RMM Statement of Facts', 7 February 2022, <https://www.justice.gov/opa/press-release/file/1470211/download>, accessed 18 April 2023.

As discussed in the case study in Box 2, Lichtenstein and Morgan first used fake identification to set up accounts. To ensure that an individual attempting to open an account with fake identification is detected, VASPs can implement the following controls:

- In addition to proof of ID and a customer photograph, there should be a biometric 'liveness' detection test during onboarding for non-face-to-face account setup. Liveness tests are used for non-face-to-face onboarding to prove identity, typically by having the customer record a video and hold the identification next to their face.
- Identify IP addresses associated with accounts and cross-refer to other accounts to assess whether they are associated with the same IP address.
- Identify whether more than one user shares the same payout address.[42]

According to the indictment, another measure that Lichtenstein and Morgan used involved shell companies and US-based financial accounts to legitimise the activity. VASPs should consider the following actions to counter this:

- To ensure the legitimacy of potential clients' companies, perform CDD and KYC checks.
- Identify the location of the institution and customer base.

42. This may not work for blockchains that use a destination tag or memo. For further details, see Abhinav Tewari, 'What are Cryptocurrency Transaction Memos?', *BSC News*, 4 July 2022, <https://www.bsc.news/post/what-are-cryptocurrency-transaction-memos#:~:text=Crypto%20tokens%20that%20require%20the,or%20Terra%20Classic%20(LUNC)>, accessed 27 June 2023.

Finally, Lichtenstein and Morgan used automated scripts to conduct multiple transactions in a short amount of time.[43] They also leveraged services in darknet markets and converted crypto assets into different cryptocurrencies, including privacy coins. Hence VASPs should consider the following:

- If trading is automated, ensure that risk controls and system safeguards are implemented, adequately designed and effective.
- Check if the incoming funds come from darknet markets.
- Identify chain-hopping between cryptocurrencies through open source platforms or blockchain analytics tools if available.

# Terrorist Financing

Terrorist groups have shown interest in VA use, but mainly for donations. These donations are typically not a product of criminal revenue streams and are sent from supporters globally. The seemingly licit nature of these transactions can create a challenge for detection unless the recipient address is correlated to a terrorist organisation. This attribution may not appear on open source transaction tracing platforms, but terrorist groups use methods that should be considered when assessing TF risk. It is important to note that these are not typologies, due to the limited availability of cases where terrorist groups abuse the VA industry. However, they should be considered as part of the assessment process.

**Box 3: Al-Sadaqah and Bitcoin Vouchers**

Al-Sadaqah, a group associated with Al-Qa'ida and claiming to be raising funds for fighters in Syria, encouraged supporters to donate cryptocurrency through two separate methods:

- Purchasing Bitcoin vouchers for a gaming website to share with Al-Sadaqah so that the terrorist organisation could access and use the funds.
- Going to a Bitcoin ATM to purchase cryptocurrency with cash and put funds on a digital or paper wallet to share with the organisation (some ATMs allow for a printed QR code on a receipt).

Source: Yaya J Fanusie, 'Survey of Terrorist Groups and Their Means of Financing', Foundation for Defense of Democracies, 7 September 2018, <https://www.fdd.org/analysis/2018/09/07/survey-of-terrorist-groups-and-their-means-of-financing/>, accessed 28 June 2023.

43. Automated trading enables traders to calibrate rules and conditions for trades that can subsequently be automatically executed with no human intervention.

As discussed in Chapter I, crypto ATMs enable cash-to-crypto transactions and occasionally vice versa. They are considered an inherently higher risk because they allow for a fiat on ramp. In regulated jurisdictions, they typically have built-in AML measures to mitigate this risk; however, it is important to verify this information:

- Ensure that the crypto ATM has robust AML/CTF/CPF controls in place.
- Ensure that the crypto ATM is licensed/registered and/or obtains a licence/registration from the regulator.

Another method that terrorist group supporters use involves NFT creation. In addition to the regulatory ambiguity of these unique tokens, there is a risk associated with their immutable nature. Once minted on the blockchain, the NFT cannot be removed, providing an opportune structure for terrorist groups to create content without the fear of it being deleted. In one case, as shown in the following case study, a supporter minted an NFT praising a terrorist organisation.

**Box 4: The Islamic State and NFTs**

In August 2022, the *Wall Street Journal* reported that a terrorist sympathiser disseminated an NFT that praised Islamist militants for an attack on a Taliban position. The content of other NFTs created by the same user included a person in a laboratory suit and gas mask surrounded by beakers and assault rifles, as well as one that condemned cigarette smoking. Although the NFT marketplace used by the sympathiser removed this content, this NFT can still be found through alternate platforms.

Source: *Wall Street Journal*, 'Islamic State Turns to NFTs to Spread Terror Message', 6 September 2022.

Whether tied to terrorist activity or fraud in general, a verification mechanism should be implemented to determine whether the incoming funds are derived from licit content:

- If the source of funds is from an NFT, verify the content of the NFT and associated collections.

# Proliferation Financing

Another typology is the creation of an initial coin offering (ICO) to obtain investments. The first case of a North Korea-linked individual launching an ICO, Marine Chain Token,[44] was in 2018. This token, which represented fractional ownership interests in marine shipping vessels, was an attempt by North Korea to evade sanctions and fund its WMD programme.[45]

While the PF case study below may not depict a direct link to the North Korean regime, it illustrates an additional case of an ICO created with the aim to support North Korea.

**Box 5: Asia-Pacific Peace Interchange Association (APPIA) Cryptocurrency**

In 2019, APPIA launched its own cryptocurrency, APP427, to raise funds that could be invested in North Korea when UN sanctions are lifted. According to TRM Labs, APPIA received approximately $800,000 from nearly 100 investors during the ICO. The blockchain analytics company also referenced APPIA's website, which noted that the token could be used 'in the event of a North Korean currency collapse; as a way to finance imports of North Korean beer; and [as] the basis for selling North Korean art as NFTs'.

Source: TRM Labs, '"North Korea Coin": The Mystery Cryptocurrency Caught Up in a South Korean Corruption Scandal', 3 February 2023, <https://www.trmlabs.com/post/north-korea-coin-the-mystery-cryptocurrency-caught-up-in-a-south-korean-corruption-scandal>, accessed 29 June 2023.

Prior to a VASP accepting new tokens on a platform, an auditing procedure that answers the following questions must occur:

- Does the token have a user guide ('white paper') documenting all relevant material, such as the commercial, technical and financial information relating to the token? Is the white paper unique or copied from another token? What is the token's purpose as listed in the white paper?
- What is the asset's regulatory status (for example, share, security, collective investment scheme) and what licensing obligation does the VASP need as a result?

44. Insikt Group, 'Shifting Patterns in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite', Recorded Future, 25 October 2018, <https://www.recordedfuture.com/north-korea-internet-usage>, accessed 5 April 2023.
45. United States of America vs. Jon Chang Hyok, Kim Il, and Park Jin Hyok, 'Introductory Allegations and Definitions', United States District Court for the Central District of California, 2:20-cr-00614-DMG, January 2020.

- Does the asset allow for the option to add anonymising features (for example, zk-SNARK security protocol)?
- Has the asset been developed within or by a high-risk jurisdiction or exchange?
- What is the background of the founder and the team launching the token? Is there transparency on who designed the coin? If not, do they respond to requests for information? What information is the adverse media screening process generating?
- To what extent is the token available on other platforms?

North Korea also uses third parties to aid in the conversion between stolen cryptocurrency and fiat currency, as illustrated in the next case study.

**Box 6: OTCs**

In 2023, the US Office of Foreign Assets Control sanctioned three individuals for aiding North Korea by converting stolen cryptocurrency to fiat currency. The following steps occurred:

- OTC traders processed multiple transactions to convert millions of dollars' worth of cryptocurrency into fiat currency.
- OTC traders used Hong Kong-based front companies to purchase goods in US dollars, and three of the four companies used the same Hong Kong address as their physical registration address.
- The front companies used the funds as payment for goods, such as tobacco and communication devices, for the North Korean regime.

Source: United States of America vs. Sim Hyon Sop et al., 'Indictment', United States District Court for the District of Columbia, 1:23-cr-00129, 18 April 2023.

OTC trading occurs without an intermediary but is typically a decentralised extension of, or makes use of, high-liquidity cryptocurrency exchanges. These services allow for the purchase and selling of cryptocurrency in large volumes. If an exchange allows for OTC trading, an institution must:

- Conduct KYC on customers identified as OTC traders.
- Request that users identified as OTC traders fill out a CDD questionnaire that specifies AFC checks.

Chapter III builds on this chapter to explain how such measures are part of a wider framework that should enable VASPs to understand their inherent financial crime risks, implement mitigating measures and manage any residual risks as per the risk-based approach (RBA).

# III. Best Practices for a Robust Compliance Framework and Risk Assessment

Recent enforcement actions indicate the importance of maintaining a financial crime prevention framework that is proportionate to a VASP's number of customers, transaction volumes, deposit size and geographical footprint.[46] This chapter provides guidance on the controls and processes to implement in order to mitigate financial crime risks. It follows the general structure of the compliance cycle, beginning with client onboarding and CDD, enhanced due diligence, screening, RA and monitoring. The chapter also touches on record keeping, employee training and screening.

In addition, where relevant, Chapter III highlights the differences in compliance frameworks between VASPs and traditional banks. For instance, during the risk assessment process, a VASP will consider risk categories that are typically not relevant to traditional banking institutions, such as those associated with cryptocurrencies.

## Client Onboarding and CDD

When a VASP onboards a client, CDD and KYC checks are performed. These processes identify and verify to whom the VASP is providing products and services. The legal persons and/or entities that are subject to CDD and KYC are customers, customers' beneficial owners, authorised signatories, or individuals with power of attorney. This is essential control mitigate ML, TF, and/or PF risks.

A similar identification and verification (ID&V) process is required for one-off transactions. In addition, regulated entities are required to collate and store the information relating to their customers. This information should be reviewed periodically to ensure that customers' information remains accurate, complete

46. New York State Department of Financial Services, "In the Matter of Coinbase, Inc., Respondent'.

and valid and that the customers' circumstances have not changed. This ensures that the business relationship with customers remains in line with the regulated entity's risk appetite and that existing controls applied to customers remain commensurate and proportionate to the customers' inherent risks.

Unlike what is traditionally observed in legacy banking, VASPs' onboarding is typically not in person. Thus, to mitigate risks, liveness tests are used for ID&V. This may require the customer to provide video footage of themselves moving, speaking and/or holding identification next to their faces. VASPs perform ID&V through such digital identification systems for all customers or for customers that represent a higher risk. However, pre-recorded videos to successfully pass liveness tests for larger cryptocurrency exchanges are found on the darknet.[47]

Furthermore, VASPs need to assess the robustness and effectiveness of these digital identification tools to determine whether they are comfortable outsourcing such processes, relying on decision outcomes, or if additional controls should be implemented to complete ID&V to the necessary required level. Indeed, there are regulatory issues that inevitably emerge as a consequence of adopting such tools. Those include personal information protection, governance, explainability and interpretability. Any institution, whether a VASP or an FI, 'needs to trust the tool it is using, the "answers" it provides'.[48] As the FATF notes, 'this is especially the case when a decision is based on a high level of automation and has a direct impact on customers'.[49] The ability to explain what happens 'in the box', from input to output, ensures decision-making transparency, which in turn preserves the institution's credibility – imperative for any organisation.

Account takeovers (whereby a criminal obtains control of an individual's online account); fraud; use of mule accounts (individuals, knowingly or not, supporting criminals by using their own accounts to transfer illegally acquired assets on behalf of a third party); and ransomware/hacking are key threats to the crypto industry,[50] as underlined by the FBI's 2022 Internet Crime report.[51]

47. Authors' interview with expert 7, 23 March 2023; expert 8, 24 March 2023; and expert 9, 27 March 2023.
48. Noémi També, 'Risk-Based and Data-Led: Can the UK's Financial Conduct Authority Meet its Ambition?', *RUSI Commentary*, 28 September 2021.
49. FATF, 'Stocktake on Data Pooling, Collaborative Analytics and Data Protection', p. 33, <https://www.fatf-gafi.org/en/publications/Digitaltransformation/Data-pooling-collaborative-analytics-data-protection.html>, accessed 15 May 2023.
50. Authors' interviews with expert 1, 21 October 2022; expert 3, 24 February 2023; expert 4, 1 March 2023; expert 5, 14 March 2023; expert 6, 21 March 2023; expert 8, 24 March 2023; and expert 10, 10 April 2023.
51. The report indicates that 'in 2022, investment scams were the costliest scheme reported to the IC3. Investment fraud complaints increased from $1.45 billion in 2021 to $3.31 billion in 2022, which is a 127% [increase]. Within those complaints, cryptocurrency investment fraud rose from $907 million in 2021 to $2.57 billion in 2022, an increase of 183%'. See FBI, 'Internet Crime Report: 2022', p. 12, <https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf>, accessed 7 May 2023.

In evaluating a customer's inherent fraud risk, there are several points to consider and actions recommended:

- Whether customer age, transaction patterns, deposits and source of wealth are commensurate with one another and the customer's profile.
- Whether the customer shares devices with other users (and whether the customer uses specific types of devices and browsers to connect to their accounts).
- Whether multiple cryptocurrency accounts at a VASP are tied to one IP address.
- Checking the language of the user via the browser or application.
- Whether the customer's email was filtered for flags indicating spam or phishing, as this may indicate higher vulnerability to, for example, scams or hacks.
- Verifying the age of the email address, as scammers are likely to create new email addresses for newly scammed accounts.
- Whether the customer's phone number is a virtual one, as this may indicate scamming or account takeover.[52]
- Checking the metadata of images that have been sent by the customer.
- Where customers use virtual private networks (VPNs) or proxies, checking the internet service provider.
- Determining variation in the customer's location, using geolocation tools.
- Checking the Bank Identification Number of the customer's card to identify potential fraud.

In addition to identifying and verifying who the customer/beneficial owner/authorised signatory is, performing CDD enables the VASP to:

- Identify customers who represent an elevated risk factor for ML, TF and/or PF (this includes, for example, identifying and applying adequate due diligence on politically exposed persons (PEPs)) and obtain additional information in higher-risk situations.
- Ensure that all customers who are onboarded are within the VASP's risk appetite.
- Understand the purpose and intended nature of the business relationship.
- Ensure that all potential customers who are not within the VASP's risk appetite are not onboarded.
- Reject and/or un-bank persons and/or entities whose due diligence cannot be executed and log suspicious activity reports (SARs) if needed.

Where customer profiles change beyond the VASP's risk appetite, the VASP will exit the client. Such decisions will be documented and escalated to relevant risk

52. Scammers and hackers use voiceover IP to receive phone calls or verification text messages.

and client acceptance committees to ensure that an adequate audit trail is available.

Tables 1 and 2 provide information on the documentation that VASPs or FIs wishing to offer VAs should collate during the onboarding of legal entities and natural persons.

**Table 1:** Onboarding Legal Entities

| Information and data required | | Suggested documentation to confirm information (Note that this list is not exhaustive and may vary across jurisdictions) |
|---|---|---|
| Identification | • Full legal name.<br>• Proof and date of incorporation. | • Government registry if applicable.<br>• Certificate of incorporation.<br>• Articles of association/ memorandum. |
| Address | • Full registered address.<br>• Main place of business (if different from registered address).<br>• Address of correspondence (if different from the above). | • Government registry if applicable.<br>• Certificate of incorporation.<br>• Articles of association/ memorandum. |
| Nature of business | • Purpose of the company.<br>• Industry the company operates in.<br>• Target customer base.<br>• Locations it operates in. | • Government registry if applicable.<br>• Company website.<br>• Other relevant internet search results.<br>• Annual reports and/or accounts. |
| Purpose of account | • Objectives and expected activities on the account such as deposits/ withdrawals/ frequency of activity.<br>• Documented rationale as to why the entity requires the business relationship. | • Discussion with customer. |

| Information and data required | | Suggested documentation to confirm information (Note that this list is not exhaustive and may vary across jurisdictions) |
|---|---|---|
| Source of wealth<br>This refers to the origin of the entire amount of wealth (total assets) of the client. The information that should be obtained should provide an indication as to the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired. | • Savings from salary (basic and/or bonus).<br>• Sales of shares or other investments/ liquidation of investment portfolio.<br>• Sale of property.<br>• Inheritance.<br>• Company sale.<br>• Company profit.<br>• Gift. | • Original or certified copy of a payslip (or bonus payment).<br>• Letter from employer confirming salary.<br>• Certified investment/savings certificates, contract notes or cash-in statements.<br>• Bank statement clearly showing receipt of funds and investment company name.<br>• Signed letter from solicitor.<br>• Certified copy of latest audited company accounts.<br>• Donor's source of wealth (requirements of evidence as stated above for each individual source of wealth and a letter from the donor confirming details of the gift). |

| Information and data required | | Suggested documentation to confirm information (Note that this list is not exhaustive and may vary across jurisdictions) |
|---|---|---|
| Source of funds<br>This refers to the origin of the funds or assets which are the subject of the business relationship between the firm and its client and the transactions the firm is required to undertake on the client's behalf (for example, the amounts being invested, deposited or remitted). The acquired information should be substantive, relevant and able to establish the fund's origin and the method/ circumstances under which the funds were obtained. | • Lawful income.<br>• Gift.<br>• Inheritance.<br>• Transaction.<br>• Sale of real estate or stock.<br>• Loan. | • Personal bank account statements for the past several years.<br>• Documents showing transfer of funds from donor to investor.<br>• Statement explaining circumstances of the gift and why the gift was made.<br>• Documentation proving donor's source of funds.<br>• Statement of relationship between the investor and the deceased.<br>• Death certificate.<br>• Documentation confirming investor's receipt of inherited funds.<br>• Certification of payment of inheritance tax if any.<br>• Evidence tracing funds from estate of the deceased to the investor.<br>• Statement explaining the relationship, the amount inherited and other circumstances concerning the inheritance.<br>• Agreement of sale.<br>• Closing statements.<br>• Bank account statements.<br>• Documents tracing funds from closing to the investor's account.<br>• Letter from accounting firm confirming sale, sale price and identity of buyer.<br>• Evaluation from a certified accountant proving the value of the business. |
| Source of crypto<br>This refers to determining the initial crypto purchase and means of transfer into the new account. | • Document that confirms the origin of crypto that will be deposited. | • Wallet addresses<br>• Proof of ownership for self-hosted wallets.[53]<br>• Review of wallet using blockchain analytics tools to determine exposure to potential high-risk wallets or service providers. |

53. A few ownership proof methods exist: visual proof (the customer takes a screenshot of their self-hosted wallet (more specifically, the withdrawal address) and sends it to the VASP that will cross check it with the address they hold); the Satoshi test (the customer will send a small amount from the self-hosted wallet to

| Information and data required | | Suggested documentation to confirm information (Note that this list is not exhaustive and may vary across jurisdictions) |
|---|---|---|
| Directorships, senior management officials, authorised representative and entity's ownership | • Directors or equivalent senior individuals.<br>• Ultimate Beneficial Owner (UBO) (25% ownership threshold for normal clients and 10% for high-risk clients). | • Government registry if applicable.<br>• Certificate of incorporation.<br>• Articles of association/ memorandum.<br>• Notarised ownership structure. |
| Proof of regulation and proof of listing | • Status of regulation with relevant regulators.<br>• Name of stock exchange/evidence of listing/ active trading status. | • Name of the regulatory body which has issued the licence.<br>• Evidence of licence such as the regulator's webpage documenting licensees or extract if register is not public or confirmation from regulator.<br>• Stock Exchange extract.<br>• Annual report. |
| Tax Identification Number (TIN) | | The TIN certification document will vary across jurisdictions. This may be a:<br>• Social Security card/National Insurance number.<br>• W-9 form.<br>• Internal Revenue Service (IRS) extract. |
| Evidence of AML/ CTF/CPF/sanctions framework | Customer relationship questionnaire which will address:<br>• Use of privacy tokens.<br>• Client business type (ISIC code[54]).<br>• Complex ownership.<br>• Country risk.<br>• Product offering (custody, settlement, trading, investment, etc.).<br>• Sanctioned individuals/PEPs. | • Copy of relevant internal policies.<br>• Name of chief compliance officer.<br>• Completed customer relationship questionnaire. |
| Customer information sharing agreement where relevant | | • Service-level agreement. |
| Blockchain analytics screening and monitoring | | • Service-level agreement. |

Source: Author generated.

the VASP, thus proving control of that address); manual signing (the customer copies a message the VASP has sent and pastes it into their wallet software, thus proving control of that address. Note, however, that not all wallets support message signing); and Address Ownership Proof Protocol (AOPP, an automated version of manual signing). See 21 Analytics, 'Self-Hosted Wallet Verification Methods: An Overview', last updated 30 March 2023, <https://www.21analytics.ch/blog/unhosted-wallet-verification-methods-an-overview/>, accessed 28 June 2023.

54. The international Standard of Industrial Classification (ISIC) system is used to group businesses by their primary economic activities.

Note that the above table does not provide information for more complex ownership structures such as trusts, funds, partnerships or charities.

In addition, the reader should note that the 'evidence of AML/CTF/CPF/sanctions framework' should be collated when an institution onboards another and/or provides a correspondent relationship. Under such circumstances, a correspondent relationship type questionnaire should be part of the process.[55]

**Table 2:** Onboarding Natural Persons

| Information and data required | | Suggested documentation to confirm information (Note that this list is not exhaustive and may vary across jurisdictions) |
|---|---|---|
| Identification | • Full legal name.<br>• Date and place of birth.<br>• Nationality. | • Government-issued passport.<br>• Identity card.<br>• Permit of residency. |
| Address | • Full residential address.<br>• Country of residency. | • Driving licence.<br>• Bank statement.<br>• Utility bill.<br>• Tenancy or mortgage agreement.<br>• Employment contract.<br>• Relevant government-issued documentation. |
| Purpose of account | • Objectives and expected activities on the account such as deposits/withdrawals/ frequency of activity.<br>• This should be supported with a rationale as to why the natural person requires the business relationship. | • Discussion with customer. |

55. Interviewee 10 indicates that such a questionnaire has been implemented within their VASP and is aligned to the Wolfsberg Correspondent Banking Relationship Due Diligence questionnaire. See Wolfsberg Group, 'Wolfsberg Correspondent Banking Relationship Due Diligence Questionnaire', <https://wolfsberg-group.org/resources>, accessed 6 May 2023. In addition, the reader should note that the Global Digital Finance (GDF) AML/KYC working group has developed an Anti-Money Laundering Due Diligence Questionnaire for Virtual Asset Service Providers, which is currently open for public consultation. See GDF, 'GDF Virtual Asset Due Diligence Questionnaire – Open for Public Consultation', <https://www.gdf.io/gdf-virtual-asset-due-diligence-questionnaire/>, accessed 6 May 2023.

| Information and data required | | Suggested documentation to confirm information (Note that this list is not exhaustive and may vary across jurisdictions) |
|---|---|---|
| Source of wealth<br>This refers to the origin of the entire amount of wealth (total assets) of the client. The information that should be obtained should provide an indication as to the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired. | • Employment.<br>• Savings from salary (basic and/or bonus).<br>• Sales of shares or other investments/liquidation of investment portfolio.<br>• Sale of property.<br>• Inheritance.<br>• Company sale.<br>• Company profit.<br>• Gift. | • Original or certified copy of a pay slip (or bonus payment).<br>• Contract confirming salary.<br>• Certified investment/savings certificates, contract notes or cash-in statements.<br>• Bank statement clearly showing receipt of funds and investment company name.<br>• Signed letter from solicitor.<br>• Certified copy of latest audited company accounts.<br>• Donor's source of wealth (requirements of evidence as stated above for each individual source of wealth and a letter from the donor confirming details of the gift). |

| Information and data required | | Suggested documentation to confirm information (Note that this list is not exhaustive and may vary across jurisdictions) |
|---|---|---|
| Source of funds<br>This refers to the origin of the funds or assets which are the subject of the business relationship between the firm and its client and the transactions the firm is required to undertake on the client's behalf (for example, the amounts being invested, deposited or remitted). The acquired information should be substantive, relevant and able to establish the fund's origin and the method/circumstances under which the funds were obtained. | • Lawful income.<br>• Gift.<br>• Inheritance.<br>• Transaction.<br>• Sale of real estate or stock.<br>• Loan. | • Personal bank account statements for the past several years.<br>• Documents showing transfer of funds from donor to investor.<br>• Statement explaining circumstances of the gift and why the gift was made.<br>• Documentation proving donor's source of funds.<br>• Statement of relationship between the investor and the deceased.<br>• Death certificate.<br>• Documentation confirming investor's receipt of inherited funds.<br>• Certification of payment of inheritance tax if any.<br>• Evidence tracing funds from estate of the deceased to the investor.<br>• Statement explaining the relationship, the amount inherited and other circumstances concerning the inheritance.<br>• Agreement of sale.<br>• Closing statements.<br>• Bank account statements.<br>• Documents tracing funds from closing to the investor's account.<br>• Letter from accounting firm, confirming sale, sale price and identity of buyer.<br>• Evaluation from a certified accountant proving the value of the business. |
| Source of crypto<br>This refers to determining the initial crypto purchase and means of transfer into the new account. | • Document that confirms the origin of crypto that will be deposited. | • Wallet addresses.<br>• Proof of ownership for self-hosted wallets.<br>• Review of wallet using blockchain analytics tools to determine exposure to potential high-risk wallets or service providers. |
| Live video authentication | • Biometric liveness detection test. | • Video uploaded via ID verification service tool. |

| Information and data required | | Suggested documentation to confirm information (Note that this list is not exhaustive and may vary across jurisdictions) |
|---|---|---|
| Tax Identification Number (TIN) | | The TIN certification document will vary across jurisdictions. This may be a:<br>• Social Security card/ National Insurance number.<br>• W-9 form.<br>• IRS extract. |

Source: Author generated.

# Enhanced Due Diligence and Simplified Due Diligence

Enhanced due diligence (EDD) refers to the additional steps an entity is required to undertake at onboarding, as well as during the business relationship with a customer, to limit or manage any higher inherent risks they pose. For example, this would apply in the case of:

- A PEP.
- A person or legal entity from a jurisdiction that is higher risk as per an institution's high-risk country list.
- A customer who trades in privacy-enhancing tokens that are more vulnerable to ML, TF and/or PF, such as privacy coins.
- A client whose corporate ownership structure is highly complex and hence opaque.

Institutions that onboard higher-risk customers need to have robust systems and controls in place to perform EDD. An institution that is unable to perform EDD on high-risk customers should not onboard them. Similarly, if a customer is onboarded as a normal or lower-risk customer and their circumstances change in a way that requires EDD to be performed, the institution needs to ensure that this is possible. If the VASP is unable to apply EDD, the client will need to be offboarded. A SAR may also need to be logged with the relevant FIU.

Where a VASP determines that EDD needs to be implemented, the following will be performed:

- Obtaining and corroborating additional KYC and CDD relating to the customer and the beneficial owner.

- Lowering the beneficial ownership percentage from 25% to 10%.
- Reviewing the KYC and CDD and, where necessary, updating it every 12 months.
- Enhancing the monitoring of the business relationship and the transaction monitoring controls performed on the customer to identify any unusual or unexpected transactions or crypto movements that may result in suspicion of ML, TF and/or PF.
- In case of a PEP's involvement within a corporate structure, documenting their role within the company.
- Performing further searches such as verifiable adverse media to enhance the understanding of the customer's risk profile.
- Obtaining additional information on the customer's intended nature of the business relationship, the reasons for and economic background of the transactions, the plausibility of these transactions, and the customer's source of funds and/or wealth to confirm that they do not constitute crime proceeds.
- Obtaining further information and evidence on the customer's tax status.
- Assessing the information provided in relation to the destination of crypto and the reasons for the transaction.
- Obtaining appropriate sign off by the relevant customer acceptance committee and/or senior management to start or continue the business relationship.
- Requesting the customer to make their first payment through an account in their name from an institution that has robust CDD/KYC processes in place.

The CDD/KYC processes and controls documented will also enable the onboarding team and senior management to identify whether customers:

- Operate accounts on behalf of third parties.
- Are involved, either directly or indirectly through relationships with third parties, in virtual asset operations within high-risk jurisdictions.
- Are involved with privacy coins.
- Use VPNs, Onion Router, encrypted, anonymous or randomly generated email addresses.
- Consistently avoid thresholds through smaller transactions.
- Send or receive VAs to/from high-risk exchanges as per the VASP's risk assessment, unregulated exchanges or sanctioned addresses.
- Have the same payment addresses as other customers who are at a higher risk of being a mule or a scam victim.
- Have the same device as other customers who are at a higher risk of being a mule or a scam victim.
- Are suspicious or display inconsistencies during the video verification process.
- Have a commercial and/or social pattern that is consistent with scammers.[56]

56. This can be verified by checking customers' social media activity and content.

Where a VASP determines that a customer represents a lower ML, TF and/or PF risk, simplified due diligence (SDD) measures may be applied. For instance, this may arise if a customer is a regulated obliged entity domiciled in a low-risk country, subject to robust AML/CTF/CPF obligations.

Under such circumstances, the following decisions may be made:

- The customer identification and verification process may be less onerous (for example, production of one form of ID instead of two).
- The purpose of the account and rationale of the business relationship may not be documented.
- The frequency of CDD/KYC updates may be reduced.
- The frequency of ongoing due diligence and transaction monitoring may be reduced.

The lower risk status of the customer needs to be reviewed yearly to ensure that their circumstances have not changed and that the conditions which allowed the application of SDD are still met.

# Screening Customers for Sanctions and Adverse Media Risks

Client screening is performed as part of the CDD/KYC process and supports determining whether a client represents an elevated risk. Screening the client will determine whether there are any matches with individuals and/or entities that:

- Have negative press.
- Have been criminally prosecuted.
- Have a controversial reputation.
- Are PEPs.
- Are relatives or close associates of PEPs.
- Are sanctioned.

Adverse media screening is conducted using third-party screening tools and is performed periodically. Sanctions screening needs to be performed daily. The screening outcome can affect the risk level applied to the customer and can trigger an EDD process and/or the offboarding of the client.

In addition, the VASP will screen all customers, beneficial owners, authorised signatories, power of attorney holders, company directors and/or all other relevant individuals as well as all intermediary structures and parties reported

on an organisation chart. The VASP should ensure that more senior staff members review customers with known and existing elevated risk factors.

# Risk Assessment Methodology

Based on the authors' research and the qualitative data collated through expert interviews, the authors have developed a risk assessment (RA) framework (Table 6) mapping risk factors against risk categories, which suggests a possible approach for determining a VASP's exposure to ML, TF and PF risks.

The RA should follow a risk-based approach (RBA) which will provide institutions with flexibility in relation to the steps they take to combat ML, TF and PF. An RBA is not a zero-failure policy and does not prevent institutions from engaging with customers or establishing business relationships that may have a higher exposure to ML, TF and/or PF risk. Rather, it guides institutions to manage and target their efforts to areas that represent higher financial crime risk.

Risk categories are listed in Table 6. They include:

- Customers.
- Wallet risk.
- Business/occupation/industry of client.
- Crypto asset token classification.
- Geographic exposure.
- Products, services and transactions.
- Delivery channels.
- Cybercrime and fraud.

Each of these categories will be assessed by reviewing their underlying risk factors (documented in the second column of Table 6) and evaluating the residual risk they represent. The reader should note that the prominence of underlying risk factors will vary across institution types. Risk factors will vary depending on the type of markets the institution services, its customers, the products it offers, delivery channels and platforms used. For example, a custodian[57] would not be expected to have the same business exposures as a CEX or a crypto ATM.

# Inherent Risks

Once risk categories have been identified, VASPs should assess their inherent risk by considering the likelihood of the risk materialising alongside the impact

57. Custodians are third parties that store and secure cryptocurrencies on behalf of clients.

of an event should it occur. Inherent risks are the financial crime risks an institution faces before considering existing controls and mitigation strategies that have been applied. This is typically assessed based on five levels of impact cross-referenced with five levels of likelihood (as documented in Table 3 below).

For example, a VASP's financial crime prevention (FCP) team may identify through a review of relevant typologies or consultation of industry reports that under the 'business/occupation/industry of client' risk category, centralised casinos that accept VAs can be used for ML. As such, the likelihood of this client being exploited for ML could be classified as 'possible' (as documented in the 'likelihood' column of Table 3). The FCP team would then judge the impact to be 'major' (as documented in the 'impact' row of Table 3), should the identified risk materialise and result in sanctions violations, reputational damage and financial losses.[58]

Cross-referencing this impact with the likelihood of this client being exposed to ML (as seen in Table 3) results in the client's inherent risk rating of 'medium–high'. The FCP team then needs to consider whether existing control measures reduce the inherent risk and generate a residual risk that is in line with the institution's tolerance or appetite, or whether additional mitigants will need to be put in place to reduce the risk of an event occurring.

58. This could be a consequence of share price drops and regulatory fines. For example, in 2019 Standard Chartered Bank paid $657 million to the US Treasury Department's Office of Foreign Assets Control to resolve sanctions violations mainly related to Iran. There were additional sanctions violations relating to Cuba, Sudan, Burma, Syria and Zimbabwe. See US Treasury Department, 'U.S. Treasury Department Announces Settlement with Standard Chartered Bank', 9 April 2019, <https://home.treasury.gov/news/press-releases/sm647>, accessed 10 May 2023.

**Table 3:** Inherent Risks

| | | Impact | | | | |
|---|---|---|---|---|---|---|
| | | Insignificant | Minor | Moderate | Major | Severe |
| | | Inherent risk | | | | |
| Likelihood | Certain | Medium–Low | Medium–Low | Medium–High | High | Extreme |
| | Almost certain | Medium–Low | Medium–Low | Medium–High | High | High |
| | Possible | Low | Medium–Low | Medium–Low | Medium–High | Medium–High |
| | Unlikely | Low | Low | Medium–Low | Medium–High | Medium–High |
| | Rare | Low | Low | Low | Medium–Low | Medium–High |

Source: Noémi També, 'Institutional Proliferation Finance Risk Assessment Guide', RUSI, 8 June 2023.

# Identifying Controls and Assessing Effectiveness

Once the inherent risk has been evaluated, the next step is to assess the institution's residual financial crime risks – namely, those that remain after existing controls and mitigation strategies to tackle inherent risks are applied.

Control effectiveness is determined by considering two elements: whether the control is well designed to mitigate inherent risks, and whether it is being adequately applied to do so. The combined operating and design effectiveness of a control indicates whether the control is ineffective, partially effective, mostly effective or effective. Determination as to whether controls are designed and operate effectively should be based on controls testing.

**Table 4:** Control Effectiveness

| | | Operating effectiveness | | | |
|---|---|---|---|---|---|
| | | Ineffective | Partially effective | Effective | Highly effective |
| Design effectiveness | Ineffective | Ineffective | Ineffective | Ineffective | Ineffective |
| | Partially effective | Ineffective | Ineffective | Partially effective | Effective |
| | Effective | Ineffective | Partially effective | Effective | Effective |
| | Highly effective | Ineffective | Effective | Effective | Highly effective |

Source: També, 'Institutional Proliferation Finance Risk Assessment Guide'.

For example, in the case of the above example where a client's industry was assessed as having a 'medium–high' inherent risk, the VASP will assess the effectiveness of the controls in place to mitigate the risks of such a client being exploited for ML purposes.

# Residual Risks: Combining the Score of Control Effectiveness with that of Inherent Risks

If controls are assessed as effective, then overlaying this assessment with the inherent 'medium–high' risk rating would result in a residual risk of 'medium–low'. It is key to note that such frameworks need to be flexible and that the expertise and knowledge of the FCP team feeds into such evaluations. The FCP team needs to apply an RBA. Indeed, despite the controls being evaluated as effective, the FCP team may estimate that the residual risk should be 'medium–high', for example, due to elements that may have not been qualitatively or quantitatively captured in the assessment. Hence, 'technical assessments performed by risk analysts can be overridden, enabling analysts to use heuristic techniques often influenced by "gut instinct", or sensitivity to a particular topic or ethics, when assessing certain risks associated with a particular event'.[59] Such factors need to be clearly documented and articulated and should be reviewed

59. Noémi També Bearpark, *Deconstructing Money Laundering Risk: De-Risking, the Risk-Based Approach and Risk Communication* (New York, NY: Springer International Publishing, 2022), p. 23.

and assessed via adequate governance arrangements (for example, a risk and audit committee) to justify the decision.

**Table 5:** Residual Risk

| | | Inherent risk | | | | |
|---|---|---|---|---|---|---|
| | | Low | Medium–Low | Medium–High | High | Extreme |
| | | Residual risk | | | | |
| Control effectiveness | Ineffective | Low | Medium–Low | Medium–High | High | Extreme |
| | Partially effective | Low | Medium–Low | Medium–High | High | Extreme |
| | Effective | Minor | Low | Medium–Low | Medium–High | High |
| | Highly effective | Minor | Minor | Low | Medium–Low | Medium–High |

Source: També, 'Institutional Proliferation Finance Risk Assessment Guide'.

# Vulnerabilities to Financial Crime Risk and Next Steps

Once the institution has completed its RA, it can measure its residual financial crime risk and vulnerabilities (in terms of potential non-compliance with regulations or too much risk exposure, for instance). Institutions can subsequently choose whether to accept, further mitigate or prevent such vulnerabilities and exposures.

They may want to strengthen and enhance existing controls to tackle the highest-rated inherent risks identified ('extreme' in Table 3), and modify other controls deemed ineffective or partially ineffective. Operating under the RBA, the objective is to target the highest identified inherent risks. In this spirit, institutions may also decide to review certain controls that may be seen as disproportionate in efforts to mitigate lower inherent risks.

Furthermore, the RA will help institutions better understand and define their risk appetite while being aligned to AFC laws and regulations. Institutions may therefore decide to review and assess their existing commercial strategies.

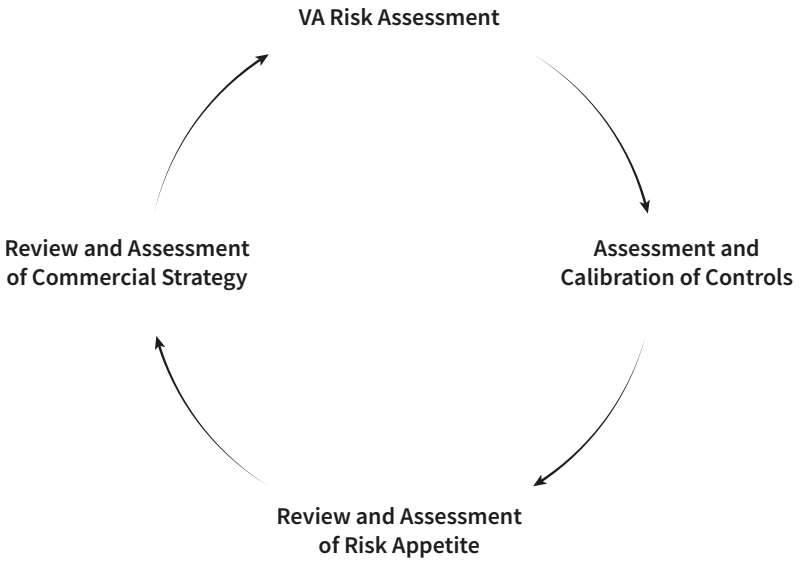
This may result in the institution:

- Stopping certain activities in certain jurisdictions.
- Terminating certain business relationships.

- Launching new commercial ventures.
- Developing governance and controls arrangements to strengthen alignment to risk appetite.

RAs should be a dynamic exercise, and the above can feed into the next RA cycle to ensure emerging and/or future vulnerabilities to financial crime are identified. This is illustrated in Figure 1 below.

**Figure 1:** The Risk Assessment Cycle




Source: També, 'Proliferation Finance Risk Assessment Guidance for the Private Sector'.

Table 6 adds to the RA methodology described above by documenting the financial crime risk categories that need to be considered. ML, TF and PF risk categories are listed there and include:

- Customer risk.
- Wallet risk.
- Business/occupation/industry of client risk.
- Crypto asset token classification risk.
- Geographical risk.
- Products, services and transactions risk.
- Delivery channel risk.
- Cybercrime risk.
- Fraud risk.

Institutions will then need to consider each risk against the risk factors relevant to their business activities. The prominence of specific risk factors will vary across institutions. A CEX, for example, would not have the same business exposures as a crypto ATM. Risk factors will vary depending on the type of markets the institution services, its customers, the products it offers, and the delivery channels and platforms used. Note that Table 6 does not provide an exhaustive list of risk factors.

**Table 6:** Risk Assessment Categories and Factors

| Risk categories | Risk factors |
|---|---|
| Customer risk | Residency and nationality (including connections to a sanctioned jurisdiction).<br>If a legal entity: country of incorporation and principal place of business. |
| | Occupation (employed, self-employed, unemployed, retired, student). |
| | Age (for example, elevated risk factor for mule accounts or for discrepancy with income and/or behaviour on the account). |
| | Salary range (elevated risk factor for discrepancies with other risk factors such as age and occupation). |
| | Sharing IP address, VPN services obtained from established or obscure vendors.[60] |
| | PEP, high-risk client, sanctioned status, adverse media hit, tax status. |
| | Transaction types (trading, investing, reselling, gambling, buying/selling goods and services, arbitrage). |
| | Source of wealth, source of crypto and purpose of account (salary, investment, gaming, mining, ICO, gambling). |
| | Deposits, size of deposits, frequency, expected size and volume of transactions. |
| | Does the client hold a 'traditional' bank account, does the client use money services businesses (MSBs) or payment service providers for making payments and transfers? |
| | Legal entity, natural person.<br>• If legal entity: company type (limited company, partnership, trust, foundation, non-profit organisation), established or managed by a professional intermediary, complex corporate structure.<br>• If legal entity: publicly listed or not.<br>• If legal entity: does the activity require regulatory licence and if so, does it have one? |
| Wallet risk | Hosted/custodial wallet or self-hosted/non-custodial wallet. |
| | Ability to top up wallet with high-risk payment types (for example, fiat cards, third-party payments). |
| | Wallet risk score as identified by blockchain analytics tools.[61] |

60. When considering geographical risk, identifying the use of all VPNs as an elevated risk factor will generate large volumes of false positives. However, blockchain analytics tools aid in identifying VPN services that are commonly used by criminal groups. To mitigate perceived risk of VPN use, phone numbers with the same country code or proof of residence can be reverified at onboarding and during ongoing due diligence.
61. For instance, conversations with analysts within blockchain analytics institutions have confirmed that there are a number of criteria used to determine the risk score of a wallet (such as a wallet's percentage of funds originating from illicit activities). The only way to mitigate risks posed by self-hosted wallets is, for example, to use blockchain analytics companies that can screen for sanctioned or high-risk wallet addresses or request 'proof' that the wallet is under the control of the individual in a manner similar to requesting proof of residency by screenshots or documents. This is hard to demonstrate.

| Risk categories | Risk factors |
|---|---|
| Business/ occupation/industry of client risk[62] | Financial services. |
| | Money-exchange businesses. |
| | Providers of non-bank financial intermediation. |
| | Casinos. |
| | Cryptocurrency ATMs. |
| | Business incorporating cryptocurrency mining. |
| | CEXs. |
| | DEXs. |
| | Mixers. |
| | Trust corporate service providers and intermediaries. |
| | High-cash business (OTC broker). |
| | NFT marketplaces. |
| | Custodial services. |
| | Decentralised autonomous organisations. |
| | Embassies/consulates. |
| | Maritime/shipping industry. |
| | Research. |
| | Manufacturer. |
| | Agricultural industry. |
| | Cannabis resellers. |
| | Adult industry. |
| | Suppliers, buyers and trading partners in WMD technology/dual-use goods/nuclear/ defence industries. |
| | For other VASPs to consider, please see Table 8 in the Annex. |

62. Consider the following factors: where are the institution and its customers based? Is the institution regulated for AML/CPF/CTF? What is the size and nature of the institution and its clients? What is the nature and scope of the institution's products and services (if a VASP, this includes types of tokens)? Does the institution operate entirely online? What potential ML/TF/PF/sanctions risks are associated with the institution's connections and jurisdictions? If a VASP, has it implemented the travel rule or not? How effectively will it manage the sunrise issue? (The sunrise issue pertains to the implementation of FATF's Travel Rule. There are challenges to implementation of the Travel Rule between jurisdictions that regulate VAs and VASPs, and those that do not. For more information, see FATF, 'Targeted Update on Implementation of FATF's Standards on VAs and VASPs'.) Does the institution support transactions from/ to non-obliged entities?

| Risk categories | Risk factors |
|---|---|
| Crypto asset token classification risk[63] | Reputational risk.[64] |
| | Traceability (anonymising features). |
| | Liquidity risk.[65] |
| | Regulatory and legal risk. |
| Geographical risk | Use of jurisdictions with no or little AML/CTF/CPF regulations in place for the cryptocurrency industry. |
| | Use of jurisdictions known to be used often by sanctioned entities. |
| | Use of jurisdictions that are subject to sanctions or embargos. |
| | Offshore financial centres and non-cooperative tax jurisdictions. |
| | Jurisdictions identified as having significant levels of corruption, organised crime or other criminal activity. |
| | Jurisdictions identified as providing funding or support for terrorist activities. |
| | High-risk jurisdictions where client holds bank accounts. |
| | Jurisdictions where the client offers services (do they have services in high-risk countries, even if they are not based there?). |
| Products, services and transactions risk | Fiat-to-crypto via a bank transfer. |
| | Cash-to-crypto via a crypto ATM. |
| | Product that facilitates the use of cash to trade with crypto. |
| | Fiat-to-crypto via a credit card or third-party transfers. |
| | Crypto trading pair with fiat currency from jurisdictions that are considered higher risk. |
| | High-value payments. |
| | Overdesk, peer-to-peer exchanges. |
| | Crypto-to-crypto. |
| | Crypto-to-fiat via a bank transfer. |
| | Use of MSB to send funds to a VASP. |

63. Type of tokens as listed in Table 7.
64. Consider the following factors: how attractive is the asset as a vehicle for ML/TF/PF (price volatility, anonymity, market capitalisation)?; regulatory status of the asset (for example, share, security, collective investment scheme); licensing obligation; technology used to support the coin; does the asset allow for the option to add an anonymising feature (for example, weak protocol)?; has the asset been developed within/by a high-risk jurisdiction or high-risk exchange?; legitimacy of the white paper connected to the token (is it a copy of a more well-known token?); background of the founder and the team launching the token (is there transparency around who designed the coin? If not, do they respond to requests for information?); adverse media.
65. A crypto asset's liquidity determines the ease, speed and costs of trading such an asset. Certain coins with low market capitalisation are illiquid. This means that a trader cannot easily exchange such coins for cash, thus making them less attractive compared to other highly liquid coins such as Bitcoin or Ether, in which traders can enter or exit positions at any time.

| Risk categories | Risk factors |
|---|---|
| Delivery channel risk | Account origination via intermediaries. |
| | VASP does not verify customers' identity or use robust means to do so, or their ability to establish and verify the customers' identity is open to doubt. |
| Cybercrime risk | Technology used for custodial services is not robust.[66] |
| | The sources of wealth and funds are related to hacking and/or ransomware. |
| Fraud risk | The sources of wealth and funds are related to fraud.[67] |
| | Transactions are related to fraud.[68] |

Source: Author generated.

# Ongoing Monitoring and Transaction Monitoring

VASPs are required to perform ongoing due diligence on the customers they have onboarded.

The frequency of the review should be determined by the customer's risk profile as per the RBA. High-risk customers will be reviewed every 12 months, while normal-risk clients will typically be reviewed every two years and low-risk accounts every three years – depending on a VASP's internal processes and appetite for ML, TF and PF risks. As part of these periodic reviews, the VASP will update all KYC information and all relevant documents including expired documentation. Any change of risk classification resulting from the periodic review will require a change in the level of CDD applied. More specifically, a client reclassified from normal to high risk will be subject to EDD and will be reviewed annually instead of every two to three years.

In addition to CDD/KYC, the VASP will review and analyse transactions throughout the course of a business relationship, including performing blockchain monitoring, to ensure that the transactions being conducted are consistent with customer profiles. The VASP will thus determine whether customers' behaviours, product use, deposits and transaction volumes are aligned with expected transactions and the nature and purpose of the business relationship and, if not, whether such activities have a robust business rationale or are suspicious.

66. For example, the use of multi-party computation technology and/or hardware security module devices.
67. This may include insider trading, market manipulation, social scamming, investment scams, Ponzi schemes, romance fraud and drainware. For further information relating to fraud, refer to the State of California Crypto scam tracker, <https://dfpi.ca.gov/crypto-scams/#Glossary>, accessed 8 April 2023.
68. This includes ICO frauds.

To corroborate the business rationale of such activities, the VASP will review, assess and perform EDD. Where applicable, queries raised and resolved, findings, and decision outcomes will be documented, retained and communicated to relevant staff (including senior management), LEAs and any other AML, CTF and CPF institutions.

Transaction monitoring can be manual or automated. However, it is essential that the process be proportionate to the size of deposits, transaction volumes, transaction frequency and/or customer base. Furthermore, VASPs should understand their transaction monitoring tools, verifying their calibration rules, scenarios, IT controls and outputs on a periodic basis.

Several red flags may trigger an alert.[69] These may be:

- Particularly complex or unusually large transactions.
- Unusual patterns of transactions which have no apparent or visible lawful purpose.
- Differences in the nature, volume or frequency of transactions in comparison to usual activity carried out by the customer or activity usually carried out in the framework of a similar business relationship.
- Fiat deposits and/or withdrawals from and to bank accounts held in a different name than the account at the VASP.
- Cumulative fiat deposits and/or withdrawals.
- Blockchain analytics monitoring alerts.
- Indicators relating to anonymity enhancement.
- Indicators relating to high-risk transaction patterns.
- Indicators relating to account creation (including CDD inconsistencies, customer profiles and sources of funds, wealth and crypto).
- Indicators related to suspicious IP addresses.[70]
- Indicators related to high-risk jurisdictions.
- Indicators related to unusual behaviours (including nested exchanges[71] or money mule[72] behaviours).

69. For further guidance, see FATF, 'Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing', 14 September 2020, <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html>, accessed 8 April 2023.
70. Indicators may be when IP addresses are concealed using certain types of VPNs (information provided by blockchain analytics tools) or when a user's location derived from the associated IP address does not match the country code of their phone number.
71. Nested exchanges can be identified through blockchain monitoring and transaction monitoring. For example, indicators of nested exchange activity may be: volume and frequency of transactions that are not aligned with expected activity and/or customer profile; accounts and addresses associated with high-risk exchanges or sanctioned exchanges (such as Suex.io).
72. There are a number of mule account indicators, including: a customer whose profession (for example, a student) does not align with the amount and frequency of transactions; users engaging in multiple large transactions with a seemingly unrelated third party, in a way that is inconsistent with expected behaviour.

- Indicators related to violations of the travel rule by a VASP.[73]
- Indicators related to specific industries (including arms, nuclear research, the adult industry, the cannabis industry, archeological artefacts, illegal wildlife trade, etc.)
- Indicators relating to incoming and outgoing transactions, such as velocity, frequency and/or volume.

# Quality Assurance

The effectiveness and quality of the checks and analyses performed by AFC risk practitioners should be reviewed, assessed and escalated to senior management. This involves assessing whether instructions, procedures and controls aimed at fighting ML, TF and PF are implemented in an appropriate and efficient manner.

Any findings relating to gaps and/or weaknesses pertaining to instructions, procedures and controls' design effectiveness and/or operating effectiveness need to be appropriately documented and escalated. An action plan for remediation of internal processes, controls and procedures needs to be defined and implemented.

# Suspicious Activity Reports (SARs)

Staff members should immediately report any alert of ML, TF or PF to compliance for new and existing clients. If the alert cannot be discounted after investigation, a SAR will be sent to the FIU as per local guidelines. In addition, staff members need to apply the rule of 'no tipping off'. The VASP is prohibited from disclosing to the client or to any other third party that a SAR has been sent to the FIU and/or that an ML, TF or PF investigation is being or may be carried out.

# Record Keeping

VASPs will maintain records for a period of five years after the termination of a business relationship or performance of a unique transaction if applicable.

73. VASPs face three challenges when identifying counterparty VASPs risk: the capability of the counterparty VASP to securely hold travel rule information; whether the counterparty VASP is tied to a sanctioned person or criminal; and the level of AFC checks conducted by the business. To counteract these challenges, FATF provides guiding questions for determining the right travel rule compliance tool providers. See FATF, 'Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers', 27 June 2023, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html>, accessed 28 June 2023.

Records will be of good quality, accessible without undue delay, complete and accurate, providing a robust audit trail for internal and/or external review and investigation.

# Employee Screening

VASPs need to implement robust hiring processes in line with relevant regulations. Potential employees will be screened to safeguard against ML, TF and/or PF. In addition, the VASP will assess potential employees' competence, good standing and integrity where possible. These will traditionally include background checks, seeking references, screening for any adverse media and reviewing social media profiles, as well as an assessment of skills, knowledge and expertise.

# Employee Training

The VASP will ensure that all relevant employees, contractors, senior management and any other relevant individuals are trained to prevent the institution from being used for ML, TF and/or PF.

All staff members are required to be trained for AML, CTF and CPF annually. Targeted training should be delivered to AML, CTF and/or CPF staff or to staff that work directly with customers or whose responsibilities expose them to financial crime risks.

Chapter III discussed the best practices for creating an AML, CTF and CPF framework to mitigate financial crime risk. The reader will have seen that there are a number of elements to a robust framework that support VASPs in mitigating financial crime risks, including:

- Governance arrangements.
- Management information.
- AML, CTF and CPF policies.
- CDD/KYC arrangements including EDD and ongoing due diligence.
- 'Know your employee' checks.
- Customer risk scoring.
- PEP, sanctions and watchlist screening.
- Ability to freeze assets of designated entities and/or nationals.
- Transaction monitoring, independent controls testing and quality assurance of existing systems and controls.
- New product approval processes, including committee decisions where applicable.

- Staff training.
- Restrictions on operating in certain markets.
- SARs.
- Business-wide risk assessments.

Maintaining a financial crime prevention framework that is proportionate to an institution's customer size, volumes of transactions, size of deposits and geographical footprint is important. VASPs should aim for proactive compliance and be focused on an RBA to effectively identify, evaluate and mitigate threats from illicit actors.

# Conclusion

While VASP compliance and regulatory guidance have increased over the last few years, there is still considerable progress to be made. The FATF expects countries to implement similar preventative measures for VASPs to those they require for traditional FIs, including appropriate supervision of the sector and licensing or registration requirements. While the FATF Recommendations are aimed at their member countries and not the VASPs themselves, country implementation of these recommendations and associated guidance has increasingly required VASPs to comply, and is expected to intensify. VASPs have the opportunity to understand what is required of the sector and proactively comply regardless of whether or not their jurisdiction has implemented the FATF Recommendations.

This guide aims to support the private sector (that is, VASPs) as well as traditional FIs that wish to support VASPs on the necessary foundation and tools for developing a robust AML, CTF and CPF framework that includes an RA. To this end, the guide suggests approaches to performing a ML, TF and PF RA; identifying ML, TF and PF risks and risk factors to evaluate the institution's vulnerabilities; and identifying mitigating controls and strategies. While this guide will provide a useful starting point for conducting an institutional RA, VASPs are ultimately responsible for analysing and applying these guidelines in a way that produces a reasonable judgement of their institutional risk. If conducted diligently, an institutional RA, as well as the information collected over the course of the process, should be a critical first step in better understanding vulnerability to ML, TF and PF; proactively addressing gaps in VASPs' AML, CTF and CPF frameworks; and mitigating the impact of ML, TF and PF activities on the crypto sector, the national economy and, more broadly, society.

# Annex

**Table 7:** Token Classification

| Type of Token | Definition |
|---|---|
| Payment/exchange crypto tokens | Pseudonymous tokens on a public blockchain that serve as a medium of exchange and store of value. |
| | Pseudo-anonymous tokens that allow an add-on option of privacy-enhancing features and serve as a medium of exchange and store of value. |
| | Anonymous tokens with privacy-enhancing features by default that serve as a medium of exchange and store of value. |
| Utility tokens | Tokens that are designed to be used within a certain blockchain ecosystem and allow access to a blockchain-based product or service. |
| Security tokens | Tokens that represent legal ownership of a digital or physical asset for investment purposes. |
| Governance tokens | Tokens that allow holders of the token to vote on decisions for a blockchain project. |
| Lending tokens | Tokens that are lent out to borrowers with a set interest rate. |
| Liquid staking tokens | Tokens that represent assets that are staked to therefore use the liquidity of the locked-up tokens. |
| Wrapped tokens | Tokens that allow for unsupported tokens to be used on decentralised finance platforms. |
| NFTs[74] | Unique, non-interchangeable tokens that represent a digital asset or ownership of a physical asset. |

74. FATF notes that NFTs can fall under the definition of a virtual asset depending on whether the jurisdiction perceives it as an investment or a collectible.

| Type of Token | Definition |
|---|---|
| Stablecoins[75] | Fiat-collateralised tokens that are pegged 1:1 to fiat currency. |
| | Crypto-collateralised tokens that are pegged to the reserves of other VAs. |
| | Non-collateralised tokens that are algorithmically pegged to an object. |

Source: Author generated.

**Table 8:** VASP Classification

| Type of VASP | Definition |
|---|---|
| CEXs | Providers that facilitate exchanges in a centralised manner between VAs and fiat currency and/or other VAs, transfer VAs, and safekeep and/or administer cryptocurrency. |
| DEXs | Providers that facilitate exchanges through smart contracts between VAs and other VAs. |
| Custodial services | Providers that safekeep and/or administer VAs and allow for the transfer of VAs. |
| Virtual asset ATMs (also known as kiosks, Bitcoin teller machines, Bitcoin ATMs, or vending machines) | Physical electronic terminals that facilitate the exchange of VAs for cash and/or the exchange of cash for VAs. |
| NFT marketplaces[76] | Marketplaces that allow for the purchase of NFTs in exchange for VAs. |
| Virtual asset payment processors | Payment processors that facilitate companies accepting VAs as a payment type. |
| Casinos | Physical or virtual gambling services that allow the use of VAs by customers. |
| P2P marketplaces[77] | Platforms that perform 'matching' or 'finding' services to conduct a P2P transaction, allowing for a VA-to-VA exchange and/or a VA-to-fiat exchange. |

75. FATF notes that stablecoins can either be considered a traditional financial asset or a VA.
76. NFT marketplaces may or may not fall under FATF's definition of a VASP and are regulated on a jurisdictional basis.
77. FATF states that arrangements, even if categorised as a P2P platform, 'may have at least some party involved at some stage of the product's development and launch that constitutes a VASP'. For more information, see FATF, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', p. 55.

| Type of VASP | Definition |
|---|---|
| Cryptocurrency mining pool | A mining pool operator can provide custodial services on behalf of the pool members, then transfer a percentage of mined funds. If custodial services are not provided, nor any other services identified in the FATF definition, then it is not considered a VASP. |
| ICO issuers[78] | Persons who participate in, or provide related financial services to, issuers' offer and/or sale of VAs through ICOs. |
| Centralised mixers | Privacy-enhancing transaction mixing services that obtain custody of customers' funds during the obfuscation process. These services make it challenging to trace the origin and destination of funds on-chain. |
| Central developer or governance body behind a stablecoin | According to FATF, this includes 'the persons involved in stablecoin arrangements that conduct or provide financial services covered by the FATF definition of a VASP. A governance body consists of one or more natural or legal persons who establish or participate in the establishment of the rules governing the stablecoin arrangement'.[79] |
| Persons who maintain control or sufficient influence over a DeFi arrangement of protocol-providing VASP services[80] | Owners or operators who 'control or have sufficient influence over assets or aspects of the service's protocol, and the existence of the ongoing business relationship between themselves and users'.[81] |
| Persons that provide VA escrow services on behalf of another person | VA escrow services include services that use 'smart contract technology that VA buyers use to send, receive, or transfer fiat currency in exchange for VAs, when the entity providing the service has custody over the funds'.[82] |
| Decentralised autonomous organisations | Token shareholder-operated, blockchain-governed organisations that collectively vote on how to achieve a shared mission. Members who maintain the organisations may be considered VASPs, depending on characteristics. |
| Other | Persons who provide brokerage services that facilitate the issuance and trading of VAs on behalf of a natural or legal person's users.<br>Persons who provide order-book exchange services and coordinate orders for buyers and sellers.[83]<br>Persons who provide advanced trading services, such as trading on margin or algorithm-based trading. |

Source: Author generated.

78. During an ICO, an issuer or promoter can offer a digital asset in exchange for fiat currency or another VA. For more information, see FATF, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers'.
79. For more information on how to identify the central developer or governance body behind a stablecoin, see *ibid*.
80. For more information on how to identify the creator, owner or operation, see *ibid*.
81. For more information on how to identify the owner or operator of a DeFi application, see *ibid*.
82. For more information, see *ibid*.
83. Order-book exchange services do not include platforms which only allow buyers and sellers of VAs to find each other, and do not carry out VASP activities.

# About the Authors

**Noémi També** is an Associate Fellow at RUSI's Centre for Financial Crime and Security Studies and an independent financial crime consultant and researcher with over 20 years of professional experience across the academic, public and private sectors. She is an Associate Professor at the Luxembourg School of Business. Her academic research interests are counter-proliferation risk, AML, CTF, cryptocurrency risk management and risk appetite measurement.

Noémi has wide international experience with a particular focus on FIUs and private banking. She has managed high-profile investigations focused on AML and delivered projects for compliance control environment, processes improvements, remediation and reputational risks management. She holds a PhD in Systems Science, where her research focused on the risk-based approach, the deconstruction of ML risk and de-risking. Prior to that, Noémi was an environmental economist. She has an MSc in Environmental Economics from University College London and a BSc in Economics and Politics from the University of Bath.

**Allison Owen** is an Associate Fellow at RUSI's Centre for Financial Crime and Security Studies. Her primary research projects focus on the policy and security dimensions of cryptocurrency and new payment methods.

Allison leads RUSI's work on cryptocurrency and counterproliferation finance, focusing on North Korea's use of crypto to evade sanctions, and provides guidance for the private and public sectors to understand and mitigate associated threats.

She holds an MA in Nonproliferation and Terrorism Studies from the Middlebury Institute of International Studies, an MA in International Affairs from MGIMO University, and a BSc in Electrical Engineering from the University of Kansas. Allison is also a certified AML specialist.