dutch
banking
association

Sector Industry Baseline

Crypto-asset Service Providers

strong banks
strong society

Context

Introduction

Crypto-asset Service Providers (CASPs) are gatekeepers to the financial system. CASPs active in the Netherlands must register with the DNB and are subject to the 'Wet ter voorkoming van witwassen en financieren van terrorisme' (Wwft) and the Sanctions Act. EU-based CASPs are also subject to: the revised 4AMLD, the Funds Transfer Regulation and as of end of year 2024 the Markets in Crypto-assets Regulation (MiCaR). This Sector Industry Baseline describes the risk-based banking practice within the current regulatory framework. Introduction of new legislation may, when relevant, lead to a revision of this document.

The Wwft describes the responsibilities and legal obligations of gatekeepers to prevent abuse of the financial system for money laundering (ML) and terrorism financing (TF). These encompass client due diligence, ongoing monitoring and reporting of unusual transactions. CASPs are required to perform the same controls and measures as financial institutions.

Crypto-assets can make transactions cheap, quick and easy and provide an opportunity to those without access to the traditional financial services sector to make payments and perform investments. Crypto-assets are increasingly used in transactions and investments, usually for legitimate purposes.

Various international organisations have stated that CASPs carry inherent ML/TF risks, recognizing the threat of criminal abuse of crypto-assets as well as its use to circumvent sanctions. Several features and particularly specific segments/services within the CASP industry make it an attractive vehicle through which criminal and terrorist funds can enter the financial system, particularly the anonymity, the global reach and speed of transactions, and cross-border nature accompanying virtual assets. Criminals also can exploit gaps in AML/CFT frameworks by moving their illicit funds to CASPs domiciled or operating in jurisdictions with non-existent or minimal AML/CFT regulations.

Banks are obligated to apply enhanced due diligence (EDD) measures when a business relationship or transaction poses a higher ML/TF risk, according to Wwft article 8 sub 1. Performing these EDD measures can, for example, lead to frequent and recurring requests for information and documentation towards the client. When Client Due Diligence (CDD) cannot be completed or potential ML/TF risks cannot be adequately mitigated, this potentially leads to restricted access to financial services, blocked accounts or even (potential) client exit.

It is essential that the client risk assessment is performed proportionate to the identified risks and taking into account the specific circumstances of the business relationship or transaction. The risk-based approach allows banks to adjust the extent and depth of CDD on a risk-sensitive basis. Obtaining additional information or evidence is only needed if it can be used to mitigate perceived risks. Thus striking an effective balance between managing and mitigating ML/TF risks while minimising client impact and unintended consequences.

To ensure a proportionate and risk relevant approach, banks need to distinguish between risks associated with CASPs in general and the risks of an individual CASP. For CDD it is necessary to assess the risks of an individual CASP including the services offered.

In this respect it is relevant to note that there are various types of CASPs, providing e.g:

- exchange services between crypto-asset and fiat currencies;
- custodial wallets for storing crypto-assets

The risks of a CASP vary and are dependent on their service offering.

In general, CASPs hold two different account types at banks:

1 account used for their operational expenses, e.g. payments for rent, salaries, etc;
2 client account used to receive and disburse fiat currencies from/to clients of the CASP. This can also be the 'Stichting Derdengelden' account of the CASP for holding client funds.

Additionally, banks will also have business relationships with clients of CASPs that transfer funds to the account of a CASP for the purchase of crypto-assets or receive funds resulting from the sale thereof.

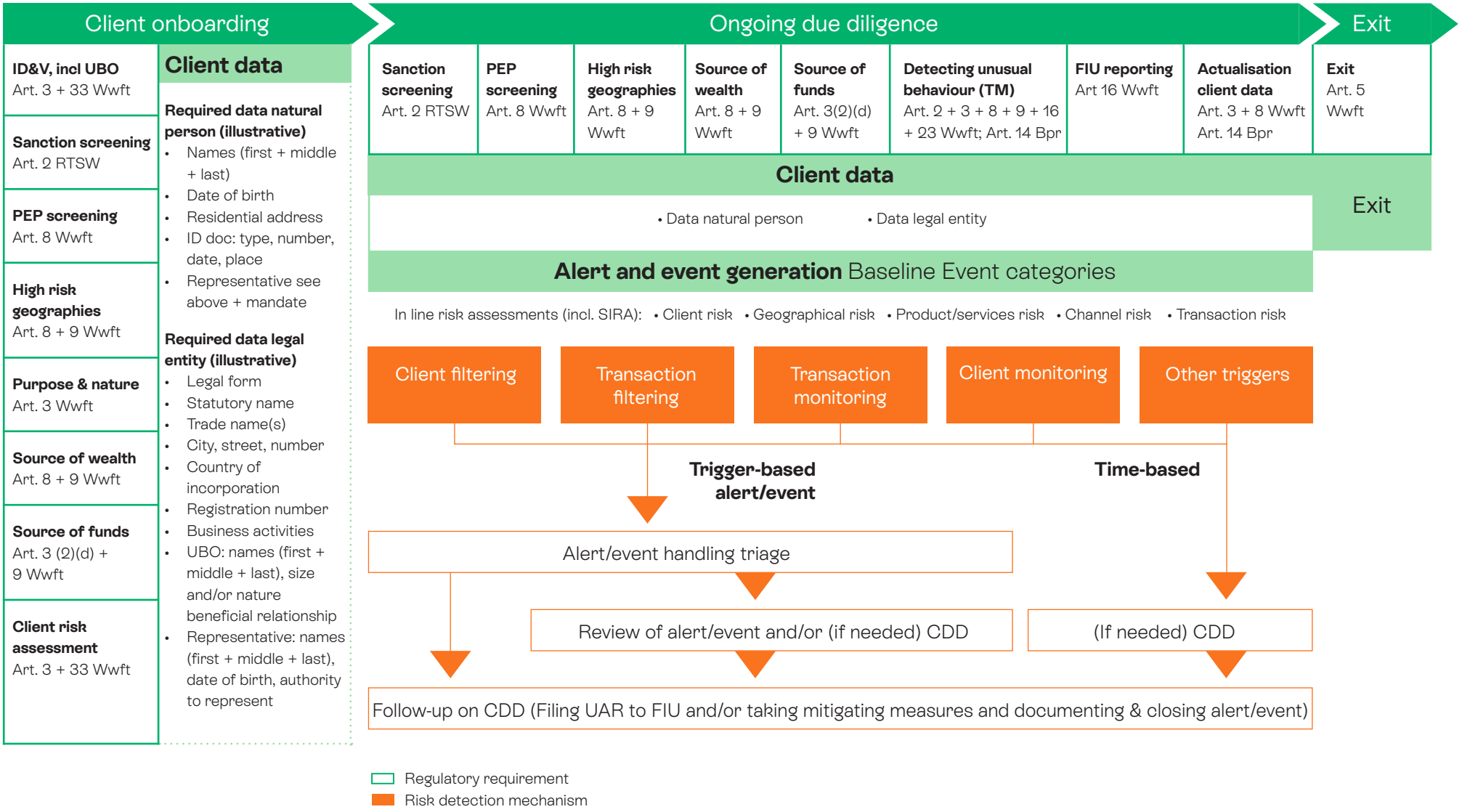
The NVB Sector Industry Baseline describes a risk-based and risk-relevant approach for implementation of CDD requirements regarding CASPs, not their clients, for various risk factors. The risk factors should be assessed case specific and interpreted in the full context of the client and the services. Based on the performed CDD and risk appetite banks decide to start and/or continue business relationships for each individual client.

Positioning within the Financial Crime Framework

The risk assessment of a CASP is part of the CDD processes. Only when a business relationship or transaction poses higher ML/TF risks.

Financial Crime Framework

Risk-based



Sector Industry Baseline

1 Industry Baseline

For both banks and CASPs, it is important that risks are assessed and controlled where needed. Risk awareness is a crucial starting point for both to achieve a proportionate risk-based approach. This means that where a risk is detected, the mitigating measures should focus on that specific risk bearing the purpose of the legislation in mind within the context of the sector.

Wwft article 8 requires banks to conduct EDD in case a transaction or business relationship by its nature poses a higher risk of ML/TF. When assessing the risks of a (prospective) client that is a CASP, banks should ensure sufficient understanding of the CASP's type and nature of their business, whether the provider is registered or licensed in an EU/EEA member state or a third country with an adequate AML/CFT regulatory regime and the extent to which the CASP applies its own CDD measures.

1.1 Risk factors

The following table provides information on characteristics and client behaviour that banks can take into account as risk-reducing or risk-increasing factors for the risk assessment of a CASP. This information also provides CASPs with more clarity on the risk factors and contribute to further awareness on possible risk mitigation.

Risk factors	Risk reducing	Risk increasing
Licence or registration	• Licence in the EU or third country	• No registration with DNB (when active in NL a DNB registration is obligatory) • No registration or licence in the EU or third country
Location	• Established in EU or country with an adequate AML/CFT regulatory regime for providers	• Established in a third country without an adequate AML/CFT regulatory regime
Governance	• UBOs residing in EU • AML/CFT policies and procedures in line with EBA and DNB regulation • Independent compliance and audit function in accordance with size and nature of the organisation • Independent audit report on AML/CFT by reliable third party	• UBOs not residing in EU • Absence of AML/CFT policies and procedures • No compliance or audit function • No independent audit report on AML/CFT available • DNB findings related to AML/CFT • Complex structure and/or involving high risk countries (e.g. transparency)
Reputation	• Positive track record • No relevant adverse media related to financial economic crime	• Linked to criminal activities, particular related to ML/TF or other financial economic crimes
Geographies	• Mostly EU clients	• Clients from countries with deficiencies in their AML/CFT regime
Transactions and services	• No cash deposits accepted • Privacy coins (e.g. Monero, Zcash, etc) cannot be used in transactions (e.g. purchase, transfer, selling, depositing and/or withdrawing) • Only exchange and/or on- and off-ramping • Only wallet services • Blockchain analysis is used to identify potentially criminal parties and patterns • Crypto-assets on custodial wallet • Services are closed-loop	• Cash deposits possible • Privacy coins (e.g. Monero, Zcash, etc) can be used in transactions (e.g. purchase, transfer, selling, depositing and/or withdrawing) • Services related to non-fungible tokens (NFTs), decentralised finance (DeFi) • No blockchain analysis in place • Crypto-assets transferred to external wallet • Services include placing of crypto-assets (e.g. Initial Coin Offerings) • Use of anonymizing techniques (e.g., AECs, mixing and tumbling services, privacy wallets)
Continuous monitoring	• Clients and transactions are subject to adequate continuous monitoring for both AML/CFT and Sanctions • Transaction monitoring according to industry standards (e.g. FATF) and recent publications • Applying blockchain analysis for transaction transparency	• Limited or no view on adequately meeting continuous monitoring requirements • No monitoring on the use of anonymising techniques (e.g. mixing)

These risk-reducing and risk-increasing factors are to be assessed in the full context of the client. Therefore, the presence of one risk factor should not solely determine the risk classification of the client. Clients always have the opportunity to provide relevant information and documentation to elaborate on the context of specific characteristics or behaviour. To continue the relationship, it is the client's responsibility to provide the bank with timely answers to questions.

1.2 Information and documentation

The following information and documentation contribute to an adequate risk assessment when establishing a business relationship with a CASP and substantiate effective mitigating measures. Important to note that this list is non-exhaustive.

- Governance and organisational structure, including UBOs, organisational chart, explanation of the structure, number of employees, compliance policies, procedures and controls, compliance and audit functions;
- DNB registration;
- AML/CFT audit reports by reliable and independent third parties;
- Geographical location of activities, clients and operations;
- Information on client portfolio;
- Expected transaction behaviour, including in- and outflow, type, size, frequency, geographies, currencies, counterparties, etc.
- CASPs often also have a 'Stichting Derdengelden' to support their activities. Unlike the CASP, the 'Stichting Derdengelden' is not registered with DNB, but should nevertheless be taken into consideration for the overall assessment within the full context of the individual CASP along with the purpose of the funds passing through the account.

1.3 Risk assessment

The abovementioned risk reducing and risk increasing factors should be considered by banks when conducting CDD for a CASP. These risk factors should be assessed in the full context of the client. Thus ensuring effective mitigation of identified ML/TF risks while safeguarding access to financial services. The risk assessment results in a risk profile of the client based on the full and integrated and composition of the ML/TF risk factors.

Examples of criteria to consider when conducting CDD for a CASP and assessing the obtained information.

- Understand the business model, including the type of crypto-assets offered, the nature of the transactions (such as trading, investing, mining) and geographic areas in which the CASP operates.
- Appraise the technological capabilities, including the effectiveness of its transaction monitoring systems and ability to track and trace transactions on the blockchain.
- Assess the effectiveness of the compliance and audit framework, including its AML/CFT policies and procedures.
- Check the regulatory status for the jurisdictions of the operations.
- Review the experience and reputation of the UBOs and senior management. This could include checking professional backgrounds, previous involvements in the crypto industry, and possible regulatory or legal issues.
- Understand the client base of the CASP, including types, geography and nature of the transactions.

2 Banks' clients purchasing or selling crypto-assets

Banks apply CDD measures appropriate for the risk profile of an individual client. When a client transfers funds to a CASP and CDD has been performed including where necessary the Source of Funds (SoF), there is no risk increasing factor resulting from the transfer to the CASP.

When in a transaction a client receives funds from a CASP which triggers a risk indicator, the SoF needs to be assessed. The NVB Industry Baseline on Source of Funds (SoF) provides guidance on the assessment of the SoF of the client. The client can provide information to the bank on the account held at the CASP showing the original

deposit and the transactions performed in the period during which the client has held or traded crypto-assets. The Wwft does not hold requirements or legal grounds for CASPs to provide information on their clients to banks.

3 Impact

In most cases client outreach will be needed to obtain the necessary information and documentation on CASPs. However, by focusing on relevant risk factors, the outreach can be proportionate to the level of potential ML/TF risks. Moreover, a focused risk-based approach is crucial to avoid unnecessary client outreach and facilitate access financial services. Also, the use of information retrieved from open sources and observed existing client and transaction behaviour limit the administrative burden.

The outlined risk factors in this Industry Baseline, can be implemented by banks in their policies, processes and controls regarding CASPs. This enables effective management of relevant ML/TF risks while ensuring that conducting CDD does not result in the blanket refusal or termination of business relationships with an entire sector.

4 Use cases

Please note that the use cases below are examples to illustrate a practical application of this Industry Baseline and not intended to be exhaustive.

Dutch CASP

Example

A Dutch CASP has been registered with DNB for more than two years. The UBOs and senior management are Dutch. There is no adverse media related to financial crime on the CASP nor the UBOs.

Industry Baseline

- Check DNB register to confirm registration.
- Check CASP's website for crypto-assets and services offered.
- Obtain CASP's AML/CFT policy and assess adequacy.
- Obtain a copy of the CASP's most recent AML/CFT audit report

EU CASP

Example

Example

A CASP has been registered with DNB for more than one year. The UBOs and senior management are residing in the EEA. The head office of the CASP is incorporated in the EEA. There is no adverse media related to financial crime on the CASP or the UBOs.

Industry Baseline

- Check DNB register to confirm registration.
- Check CASP's website for crypto-assets and services offered.
- Obtain CASP's AML/CFT policy and assess adequacy.
- Obtain a copy of the CASP's most recent AML/CFT audit report.
- Assess the AML/CFT controls and understand the client base of the CASP in an interview with the responsible Compliance officer.

International CASP

Example

A CASP has been registered with DNB for more than one year. The UBOs and senior management are not residing in the EEA. The CASP is globally active.

Industry Baseline

- Check DNB register to confirm registration
- Check CASP's website for crypto-assets and services offered.
- Obtain CASP's AML/CFT policy and assess adequacy.
- Obtain a copy of the CASP's most recent AML/CFT audit report.
- Assess the AML/CFT controls and understand the client base of the CASP in an interview with the responsible Compliance officer.
- Interview with the Internal Audit department on the effectiveness of the CASP's AML/CFT control framework.

International CASP

Example

A CASP has been registered with DNB for less than one year. The UBOs and senior management are not residing in the EEA. There have been relevant regulatory findings, e.g. DNB has issued a fine.

Industry Baseline

- Check DNB register to confirm registration
- Check CASP's website for crypto-assets and services offered.
- Obtain CASP's AML/CFT policy and assess adequacy.
- Obtain a copy of the CASP's most recent AML/CFT audit report.
- Assess the AML/CFT controls and understand the client base of the CASP in an interview with the responsible Compliance officer.
- Interview with the Internal Audit department on the remediation of the identified deficiencies.
- Optionally a work visit to the CASP.

Context

Regulatory framework

The regulatory context for this topic is described in relevant parts of applicable laws, regulations and guidelines from various authorities, such as: FATF, EBA, Ministry of Finance and DNB. Below an overview of the current regulatory framework with reference to CASPs.

- **FATF definition**
  "Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
  i. exchange between virtual assets and fiat currencies;
  ii. exchange between one or more forms of virtual assets;
  iii. transfer of virtual assets;
  iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
  v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."
- **FATF Recommendation 15**
  "To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations."
- **FATF Recommendation 16 (i.e. the travel rule)**
  "Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers".
- **EBA Draft Guidelines amending Risk Factor Guidelines (EBA/CP/2023/11)**
  "9.20 When entering into a business relationship with a customer who is a provider of services in a crypto-assets ecosystem established in a third country, which is not regulated under the Markets in Crypto-Assets Regulation or under any other relevant EU regulatory framework, banks may be exposed to increased risk of ML/TF. Banks should carry out the ML/TF risk assessment of these customers and, as part of this, banks should also consider the ML/TF risk associated with the specific type of crypto-assets.
- **Markets in Crypto-assets Regulation**
  'Crypto-asset service' means any of the following services and activities relating to any crypto-asset:
  (a) providing custody and administration of crypto-assets on behalf of clients;
  (b) operation of a trading platform for crypto-assets;
  (c) exchange of crypto-assets for funds;
  (d) exchange of crypto-assets for other crypto-assets;
  (e) execution of orders for crypto-assets on behalf of clients;
  (f) placing of crypto-assets;
  (g) reception and transmission of orders for crypto-assets on behalf of clients;
  (h) providing advice on crypto-assets;
  (i) providing portfolio management on crypto-assets;
  (j) providing transfer services for crypto-assets on behalf of clients;
- **Wwft article 8(1)**
  "An institution shall, in addition to Article 3(2) to (4), conduct enhanced customer due diligence in at least the following cases:
  a. if the business relationship or transaction by its nature poses a higher risk of money laundering or terrorist financing."

Alignment between ‘DNB Good Practices’ and ‘NVB Sector Industry Baseline’

DNB aims to illustrate its supervisory practices to the benefit of supervised entities by, for example, providing an interpretation of regulatory requirements (Q&As) and examples on how regulatory requirements can be met (Good Practices). It is important to note that neither the DNB Q&As nor Good Practices are legally binding. DNB also provides information on the registration requirements and supervision of CASPs [1].

The NVB Industry Baseline describes the application and execution of the risk-based approach for CASPs in more detail. It results from the collaboration between the sector, banks and AML supervisor to provide more clarity and consistency based on the risk-based approach in current legislation. Additionally it provides more practical examples with risk factors and mitigating measures for various scenarios.

1 https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-sectors/crypto-service-providers/registration-of-crypto-service-providers/ https://www.dnb.nl/en/public-register/register-of-crypto-service-providers/?p=1&l=10&rc=V1dGVEFD

Dutch Banking Association
Gustav Mahlerplein 29-35
1082 MS Amsterdam
www.nvb.nl