LEGAL GUILD

Open Web Sandbox AML/CFT Risk Assessment & Recommendations

INDEX

DISCLAIMER

NO ATTORNEY-CLIENT RELATIONSHIP OR LEGAL ADVICE: Communication of information by, in, to or through this Use – Case and your receipt or use of it (1) is not provided in the course of and does not create or constitute an attorney-client relationship, (2) is not intended as a solicitation, (3) is not intended to convey or constitute legal advice, tax advice or financial advice and (4) is not a substitute for obtaining legal advice from a qualified attorney.

This document was last modified in January 2022 and is subject to change pursuant to new information and developing laws.

1. Introduction

The objective of this document is to perform an initial AML/CFT (Anti Money Laundering and Counter Financing of Terrorism) risk assessment for OWS.

This document is a collection of best practices and recommendations based on current Open Web Sandbox (OWS) operations, and as the result of conducting a risk assessment on the activities of the community. The resulting level of potential exposure may result, depending on the operational jurisdiction, on a specific obligation or requirement to implement a specific control.

The goal of this analysis is intended to work as a model for any interested party to assign a risk level to an activity and to conduct their own risk assessment procedure.

This document is a living document that will be regularly updated by the NEAR Legal Guild. It also relies on members of the community to raise relevant requests for clarifications and modifications, so please interact with us!

If there are any questions, comments, or concerns that you would prefer to not share publicly, please contact the Legal Guild (info@nearlegal.com)

What is OWS?

The Open Web Sandbox (OWS) operates as an open-source community within the NEAR ecosystem, setting up a common space for contributors, projects, and teams to collaborate and work on different initiatives across the ecosystem for rewards in USD and an equivalent is paid out in the native token - $NEAR. Like other ecosystems where value is transferred from one party to another, there exists a risk of money laundering, terrorist financing, international sanctions violations, and other compliance risks (e.g., tax evasion).

Why a risk assessment?

1) Analyze vulnerability to money laundering and related risks
2) Establish minimum controls to mitigate risks
3) Comply with laws and regulations
4) Reduce operational and reputational risk

How will we assess the risks?

Based on quantitative and qualitative data, specific risks will be rated according to the following scale:

- Low risk: 
- Medium risk:
- High risk: 

What will be the outcome?

This risk assessment will help to establish the next steps in order to manage the identified risks.

2. AML/CFT Risk Assessment

2.1 Activity, products & services 

The Open Web Sandbox (OWS) has been built to encourage participation and collaboration on different activities in the NEAR Ecosystem allowing its members to actively engage with their own activities and other opportunities enlisted by the community.

Through the OWS rewards and opportunities program (for details see Annex II) users can engage with the rest of the community and explore opportunities made available by them or the OWS. As a registered contributor, at the end of the month, the member can claim rewards for each of the activities he/she worked on. This will be evaluated by the OWS Council and the contributor receives rewards in $NEAR.

As OWS pays out rewards (originated from the NEAR Foundation and of limited value) and is not a receiver of funds, the AML risk can be considered as low. There is a higher risk, although still considered **low risk**, for terrorism financing and international sanctions violation.

2.2 Systems and channels for payments, movement, and exchange of funds

All rewards to contributors are paid out through the Sandbox SputnikDAO (Astro DAO) in line with the core values of the NEAR Ecosystem: transparency and decentralization. Each month contributors have to create a post on the NEAR governance forum to describe their achievements and calculate the rewards base.

The account details of the wallet of each contributor is publicly available and include the wallet balance and incoming/outgoing transfers.

Due to the transparency of the system (for contributors, sandbox moderators, and any third-party in general) for paying out contributors the residual risk associated is considered **low**.

2.3 Customer/third-party profile 

The main customers/third-party of OWS are the contributors who receive rewards. The contributors are generally individuals, physical persons, which have a **lower risk** associated than legal persons, as it is easier to establish the beneficial owner. Nevertheless, OWS has only limited information on its contributors.

2.4 Behavior of customers which can pose a greater AML/CTF risk

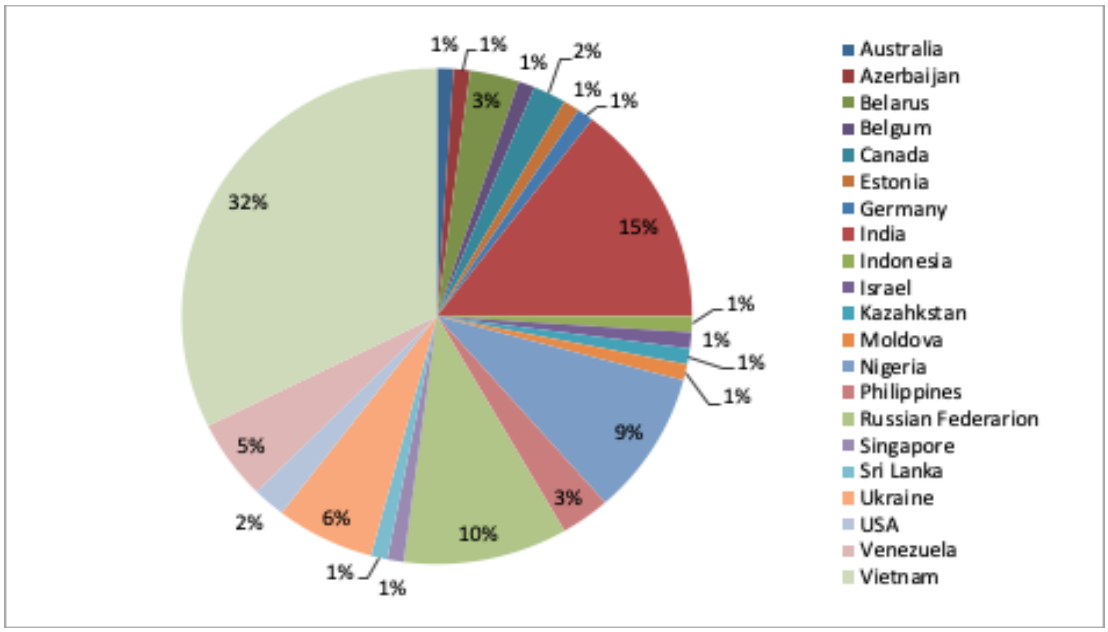
As detailed above, the AML risk is considered as low. The risk of terrorism financing and international sanctions violations is higher. Indeed, contributors could:

- Provide fake, stolen, or incorrect data
- Create multiple accounts
- Be located in high-risk territories

Because of the aforementioned points the risk related to the behavior of customers can be considered **medium**.

2.5 Geographical activity ⚠

As a decentralized community OWS operates globally. Locations of OWS contributors (as of December 2021) are:



The highest risk countries such as Iran, Syria, and North Korea are not represented in the chart. However, countries such as the Russian Federation, Ukraine, Nigeria, Philippines, and Venezuela can be considered to have a higher risk associated due to international sanctions. This risk can be mitigated by identifying contributors (e.g., asking for full name and date of birth) and cross-checking against international sanctions lists.

Considering the current situation, the associated risk with the geographical activity of OWS can be considered **Medium**.

To further reduce the risk OWS should consider defining a country risk rating based on FATF lists (see Annex I "High-risk and other monitored jurisdictions") and use geo-blocking using the country of residence declared as well as IP address.

2.6 Other AML/CTF risk factors 

No other AML/CTF risks have been identified. However, a related risk, tax compliance, has been identified. Although the final responsibility to comply with local tax regulations (which varies a lot from one country to another) depends on the contributors who receive funds, OWS should take into account this risk and limit its responsibility. Considering the current situation, the associated risk can be considered **low**.

3. Conclusion

As the overall risk is estimated as low to medium (and mainly related to sanctions) it is considered to be sufficient to implement a limited number of recommendations (see Chapter 4) without the need for a formal KYC (Know Your Client/Contributor) Policy nor AML/CTF transaction monitoring, designate an AML/CTF representative, etc.

The summary of the previous sections and the overall risk assessment is the following:

Sections Analyzed	Main Risk Factors identified	Residual Risk
2.1 Activity, products and services	Terrorist Financing and International sanctions violation	⚠
2.2 Systems and channels for payments, movement and exchange of funds	N/A	⚠
2.3 Customer/third-party profile	Contributors who are legal persons	⚠
2.4 Behavior of customers which can pose a greater AML/CTF risk	Provision of fake or incorrect data	⚠
2.5 Geographical activity	Contributors from higher-risk countries such as the Russian Federation, Ukraine, Nigeria, Philippines and Venezuela	⚠
2.6 Other AML/CTF risk factors	Tax compliance	⚠
Overall Risk: Low to Medium		⚠⚠

4. Next Steps

To properly manage the identified risks in this initial risk assessment we propose the following recommendations to be analyzed by OWS:

No.	Recommendations
1.	Use geo-blocking to block contributors from highest risk countries (see Annex I "High-risk and other monitored jurisdictions")
2.	Perform a sanction check of contributors (full name and date of birth) to ensure they are not sanctioned*
3.	Assign a responsible for performing sanction checks prior to payout to contributors

***** Consider checking against the following sanctions lists:

- Office of Foreign Assets Control (OFAC - US Department of the Treasury) economic and trade sanctions: https://sanctionssearch.ofac.treas.gov/
- United Nations (UN) Sanctions List: https://www.un.org/securitycouncil/content/un-sc-consolidated-list#individuals
- EU financial sanctions list: https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions
- UK sanction lists: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

Currently there is a free tool available online to check for sanctioned individuals on the above and other sanction lists with one search only: https://namescan.io/FreeSanctionsCheck.aspx

5. About This Document

The content of this document is licensed under a Creative Commons license:

Attribution 4.0 International (CC BY 4.0)

This is a human-readable summary of (and not a substitute for) the license. Disclaimer.

You are free to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material
- for any purpose, even commercially.
- The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- Attribution - You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use

- No additional restrictions - You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Notices:

- You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation.

- No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material.

You may need to get additional permissions before using the material as you intend.

EDO BAKKER

Team Core

SANTIAGO CHAMAT

Executive Director

Annex I: High-risk and other monitored jurisdictions

A. High-Risk Jurisdictions:

- Democratic People's Republic of Korea (DPRK)
- Iran

B. Jurisdictions with strategic deficiencies:

- Albania
- Barbados
- Burkina Faso
- Cambodia
- Cayman Islands
- Haiti
- Jamaica
- Jordan
- Mali
- Malta
- Morocco
- Myanmar
- Nicaragua
- Pakistan
- Panama
- Philippines
- Senegal
- South Sudan
- Syria
- Turkey
- Uganda
- Yemen
- Zimbabwe

Annex II: OWS rewards and opportunities program

A. **The process to access the OWS server and join the community** operates as follows:

1. To be included in the database as a contributor, the user needs to fill in the Contributor Form https://airtable.com/shr4is9xLFYTgjUmX with the following information:

   - Full Name
   - Email
   - Discord Handle
   - NEAR Wallet Address
   - Country of residence
   - Language's skills
   - Skills
   - Other Skills
   - Familiarity with Crypto and Blockchain
   - How did the user find about the Sandbox
   - Suggestions/comments

2. The user can start engaging with the rest of the community and exploring opportunities made available by them or the OWS.

3. At the end of the month, the member has to fill out a form claiming the reward for each of the activities he/she worked on. This will be evaluated by the OWS Council and sent to the NEAR wallet address that the member provided within the first week of the next month to receive the concrete reward in USD and an equivalent is paid out in the native token - $NEAR.

4. Rewards are divided between acts and series. An act is something that the member can do on its own – a series is something the member will probably need to do in collaboration with a team.

5. The reward's total amount depends on the concrete work delivered. Additionally, the OWS moderators reserve the right to decline the payout request should they, at their sole discretion, deem any submitted content not to be in compliance with the guidelines listed here

B. The OWS system for issuing rewards and paying for contributions

All rewards can be found in the OWS website

https://docs.openwebsandbox.org/earn/payment-request-guideline

C. Types of rewards and Opportunities paid by the OWS

The catalog of rewards and payments changes monthly and can be consulted in the NEAR governance forum.

Types of rewards and Opportunities paid by the OWS (as of January 2022):

For the rolling opportunities:
https://www.openwebsandbox.org/projects-dashboard

For projects in OWS:
https://www.openwebsandbox.org/projects-dashboard