

NEROBLANKO TECH B.V.

Customer Risk Assessment Procedure

Version:	1.0
Last Update:	2024-09-26
Applicability:	Neroblanco Tech B.V.
Owner:	MLRO
Approver:	CEO
Security Class:	Internal

Revision History

Version	Date	Author	Comment
1.0	26.09.2024	MLRO	First version
1.0	26.09.2024	CEO	Approval

Table of Contents

1. INTRODUCTION	4
2. CRA PROCESS	4
2.1. Timing of the CRA	4
2.2. Customer Risk Levels	5
2.3. Mandatory High-Risk Situations	5
2.3.1. Politically Exposed Persons (PEPs)	5
2.3.2. Sanctioned Individuals	7
2.3.3. High-Risk and Non-Reputable Jurisdictions	7
3. Customer Risk Matrix	9

1. INTRODUCTION

This Customer Acceptance and Risk Assessment Procedure (the "Procedure") is designed to ensure that the Company complies with the applicable laws and regulations with regards to customer acceptance and customer risk assessment.

This Procedure forms an integral part of the Company's AML Compliance Program. It should be read in conjunction with the Company's AML, CFT and CFP Policy (the "AML Policy").

Terms not otherwise defined herein have the same meaning as in the AML Policy.

2. CRA PROCESS

Customer Risk Assessment is an assessment of the particular risks the Company is exposed to in entering into or continuing its business relationship with specific customers, which is based both on the outside information collected on the customer and the history of the Company's business relationship with them.

The information thus collected is used to draw up the CRA (and the CRA itself) will compose the customer risk profile.

Company's employees and agents need to remain vigilant and use their experience and common sense in applying the Company's risk-based criteria and rules, seeking guidance from their MLRO.

On the basis of the CRA, the proper level of CDD can be applied, as detailed in the AML Policy.

2.1. Timing of the CRA

The initial CRA is carried out immediately upon the first account review, based on the information collected so far through the CDD measures.

Thereafter, the CRA is regularly updated if new information indicates a change in the risk level:

- During account reviews performed by the Company,
- When an automatic red flag is raised by the back-office software,
- When ongoing monitoring identifies a material change in the customer's profile or behavior.

PEP and Sanctions screening is performed upon player account registration using the specialized software. The screening is performed each time the CRA is thereafter performed.

2.2. Customer Risk Levels

The AML Policy recognizes three types of customer risk level:

- Unacceptable Risk
- Low Risk
- Medium Risk
- High Risk

Identifying a customer as presenting a high-risk of ML/FT/FP does not necessarily mean that the customer is involved in ML/FT/FP.

On the other hand, identifying a customer as carrying a lower risk of ML/FT/FP does not mean that the customer presents no risk at all.

In certain situations, the level of risk posed by a customer is deemed Unacceptable, which means that the Company will not establish / terminate the business relationship with the customer.

2.3. Mandatory High-Risk Situations

There are certain instances in which any customer is deemed high-risk, regardless of all other factors and of any other aspect of their risk profile. These customers will remain high-risk until the relevant circumstances change.

The procedure and the obligations related to the mandatory high-risk situations is an important part of every AML/CFT/CFP training.

2.3.1. Politically Exposed Persons (PEPs)

Relationships with PEPs may represent increased risks due to the possibility that individuals holding such positions may misuse their power and influence for personal gain or advantage, or for the personal gain or advantage of close family members and close associates.

Such individuals may also use their families or close associates to conceal funds or assets that have been misappropriated as a result of abuse of their official position or resulting from bribery and corruption. In addition, they may also seek to use their power and influence to gain representation and/or access to, or control of, legal entities for similar purposes.

Certain PEPs in certain positions may also be exposed to the possibility of being involved in FT/FP.

A “politically exposed person” (PEP) is a natural person who is or has been entrusted with a prominent public function, other than middle ranking or more junior officials, for the duration of their function up and until one year after they leave office (while in the case of family members and associates, these are no longer considered as PEPs immediately after the PEP leaves office), including the following individuals:

- 1) Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries,
- 2) members of Parliament or similar legislative bodies,
- 3) members of the governing bodies of political parties,
- 4) members of the superior, supreme, and constitutional courts or of other high level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances,
- 5) members of courts of auditors, or of the boards of central banks,
- 6) ambassadors, chargé d'affaires and other high-ranking officers in the armed forces,
- 7) members of the administrative, management or supervisory boards of state-owned enterprises, or
- 8) anyone exercising a function equivalent to those set out in paragraphs (1)-(6) above within an institution of the European Union or any other international body.

This list is by no means exhaustive and when deciding if a particular customer could be considered as a PEP, the jurisdiction, type, size, budget, powers and responsibilities associated with a particular public function have to be taken into consideration.

The family members of a PEP are subject to the same procedures as the PEPs themselves. These generally are (but are not limited to):

- 1) the spouse, or any person considered to be the equivalent to a spouse,
- 2) the children and their spouses, or persons considered to be the equivalent to a spouse, and
- 3) the parents.

The Company considers PEPs, their family members and close associates as high-risk customers. In order to mitigate risks associated with PEPs, the following measures are taken:

- 1) The CRA for the PEP customer is to be performed by the MLRO. The assessment should include information from external providers, publicly available information (online and media search), assessment of geographical risks and any other background information,
- 2) Once the CRA is completed, the CEO is notified by the MLRO, in order to obtain the CEO's approval for this particular relationship. Based on provided information and recommendations by the MLRO, the CEO will decide whether the company approves the establishment and/or wants to continue business relationship with a PEP customer.
- 3) The EDD measures are applied based on the CRA, but at a minimum, the SOW and SOF are verified,
- 4) Enhanced on-going monitoring of the activities in the account. The information of the

customer and account must be entered into “Enhanced On-going Monitoring-PEPs” spreadsheet and checked daily until risk level is decreased or a decision has been made that less frequent checks are sufficient, and

- 5) All searches, reports and decisions undertaken by employees should be duly documented and retained on the shared drive. Additionally, any decisions taken must also be documented within the player’s profile within the back-office software.

2.3.2. Sanctioned Individuals

All customers are screened against sanctions lists of the UN and EU. If Curaçao publishes a local list with designated persons and organizations, the Company shall also take that local list into account.

This screening is performed upon account opening - before the business relationship is established - and is periodically repeated thereafter when the account is reviewed.

Screening includes a check of the published lists of known or suspected terrorists or other sanctioned persons or companies:

- U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List Specially Designated Nationals and Blocked Persons List (SDN),
- Lists I Office of Foreign Assets Control (treasury.gov),
- EU Sanctions List <http://www.sanctionsmap.eu/ft/main>.

If a sanctioned individual is detected, the business relationship shall not be established. In the case of existing relationship, the account shall be closed and all funds shall be frozen, pending the UTR and further instructions from FIU.

2.3.3. High-Risk and Non-Reputable Jurisdictions

The company is required to have procedures in place to manage the risks posed by the countries and geographical areas where it operates and/or is exposed to as a result of its business activities. The jurisdictions where the company is offering its services or from where it receives money must be assessed on whether they are to be regarded as non-reputable or high-risk.

A non-reputable jurisdiction is one that has deficiencies in its national AML/CFT/CFP regime or has inappropriate and ineffective measures for the prevention of ML/FT/FP. A high-risk jurisdiction is a wider term, and other factors must be considered, for example:

- Level of Transparency and Freedom of the Press
- Level of Corruption
- War-torn countries/Civil unrest
- Significant level(s) and type(s) of crime(s) – jurisdictions known for high level of different type of crimes, including drug trafficking, arms trafficking, human trafficking

- Significant level of terror threat
- Recent escalations/events which may change the classification of a jurisdiction from a low to a high-risk jurisdiction.

While a non-reputable jurisdiction is always to be regarded as a high-risk jurisdiction, a high-risk jurisdiction may not necessarily always be regarded as a non-reputable jurisdiction.

There are several sources which determine the list of non-reputable jurisdictions:

- Financial Action Task Force (FATF) Public Documents,
- European Commission Delegated Regulations (EU),
- Statements and/or Declarations issued by the FATE, CFATE, or by another FATF-style regional body.

The law does not prohibit the establishment of a business relationship with customers from non-reputable jurisdictions but requires the application of commensurate EDD measures, targeted to mitigate ML/FT/FP risks associated with a particular jurisdiction.

3. Customer Risk Matrix

Risk Level	Customer	Geo	SOF / SOW	Transaction
Unacceptable Risk	Sanctioned individual A customer that does not comply with the Company's CDD requirements Anyone deemed to be linked with ML/TF/PF Company officer, employee or agent	Residents of Prohibited jurisdictions Residents of FATF's "blacklist" jurisdictions.	Cash income Funds appear to be generated or linked to the proceeds of crime	A customer that does not comply with the Company's CDD requirements
High Risk	PEP customers Customers with links to crime or under investigation Customers who were subjects of adverse media Customers who are or have been subjects of a SAR or internal investigation Customers who provide fake, stolen or	Residents of high-risk or non-reputable jurisdictions	Use of over 5 different payment methods	Customers who reach 10000 EUR or equivalent of transactions within 24 hours Customers who reach 75000 EUR or equivalent of transactions within 1 month Customers with transactions, which are complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose

	altered documentation Professional gambler, sport industry professional or involved in a cash-heavy industry			
Medium Risk	Customers suspected of illicit activities such as registering duplicate accounts or using payment methods belonging to their third parties (pending further investigation) Customers with links or similarities with other medium/low risk customers Any other customer, determined by the MLRO / AML team as medium risk	Countries which in the opinion of the MLRO represents heightened risk	Use of up to 4 different payment methods	Customers who reach 2000 EUR or equivalent of transactions within 1 month
Low Risk	All of the customers are considered Low risk after a sign up until they meet any of the Medium/High risk criteria	Fully compliant with FATF No AML/CTF concerns	Bank transfer Debit or credit card Approved payment service provider	Under any of the qualifying payment thresholds