

Risk Management Policies and Procedures for Crypto Use of SEVENTORIA B.V.

Objective

SEVENTORIA B.V. applies blockchain-based solutions to support cashless gameplay and digital wallet operations within its online gaming environment. All cryptocurrency transactions are protected by security protocols and AML/CTF controls. The company maintains a structured risk management framework to safeguard assets and reduce the risks associated with virtual assets.

Scope

This policy covers all employees, business units, and affiliated entities of SEVENTORIA B.V. involved in using, managing, or monitoring cryptocurrency transactions and services.

1. Risk-Based Approach (RBA)

1.1. Definition

The company follows a Risk-Based Approach (RBA) to evaluate and mitigate risks tied to the use of cryptocurrencies. This involves the ongoing process of identifying, assessing, and applying suitable measures to control those risks.

1.2. Risk Identification

The company reviews and records potential risks linked to crypto transactions, including:

- market fluctuations,
- liquidity risks,
- cyber and information security risks,
- regulatory and compliance risks,
- operational and process risks.

Tools such as internal checklists, risk registers, and structured risk assessment sessions are used to ensure no significant area is overlooked.

2. Risk Analysis

2.1. Detailed Risk Analysis

After identifying risks, we analyze each risk in detail by:

- Assessing the likelihood of each risk materializing and its potential impact.

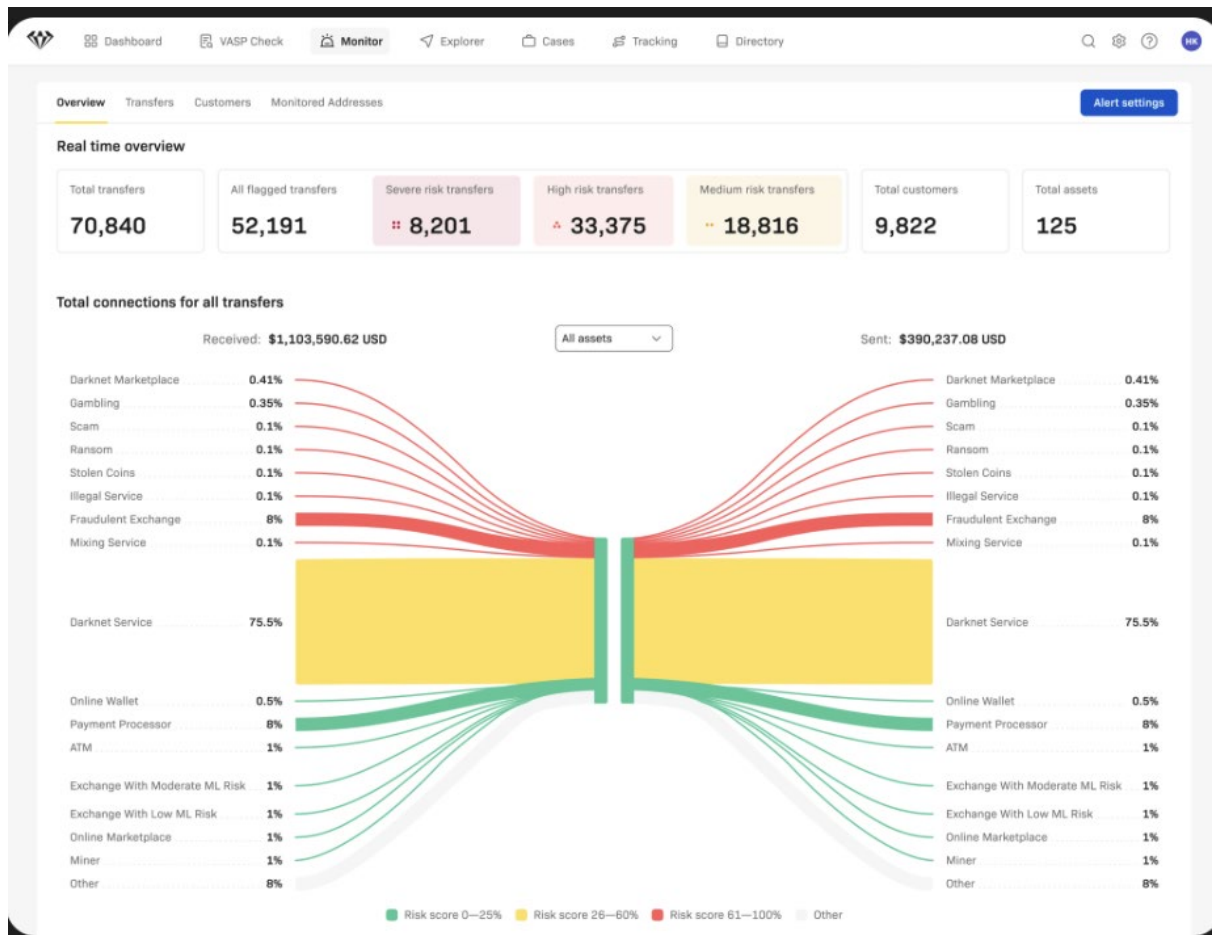
- Employing quantitative and qualitative techniques such as scenario analysis, stress testing, and sensitivity analysis to evaluate the potential impact and effectiveness of various risk mitigation strategies.

2.2. Transaction Monitoring

Pattern Analysis. Our monitoring system focuses on in-game play, deposit frequencies, and transaction patterns rather than solely on the amounts deposited or withdrawn. We scrutinize account activity for unusual sizes, volumes, patterns, or types of transactions, using red flag indicators to detect suspicious behavior.

Chainalysis Review. Every crypto deposit or withdrawal, whether direct or indirect, is processed through Chainalysis and reviewed for signs of fraud or suspicious activity. If potential illicit behavior is detected, the user's account will be suspended and subject to further review. High-risk accounts may be required to provide sufficient proof of wealth. Additionally, we may refuse withdrawals to certain “high-risk” addresses based on Chainalysis risk scoring.

Crystal Platform. This transaction monitoring establishes the framework for monitoring and analyzing cryptocurrency transactions within our organization. Effective transaction monitoring is crucial for detecting fraudulent activities, ensuring compliance with regulations, and safeguarding against financial crimes. The monitoring is supported by the **Crystal platform**, which provides scalable and flexible tools for crypto investigations.



3. Due Diligence Measures

3.1. Customer Due Diligence (CDD)

Blockchain analysis tools are applied to monitor the source of funds for any cryptocurrency transaction and indicate if a wallet address has been exposed to fraudulent behavior or suspicious sources.

3.2. Enhanced Due Diligence (EDD)

Enhanced due diligence is carried out for high-risk clients and transactions, particularly those involving significant amounts or unclear sources of funds.

3.3. Account Blocking and Freezing

Accounts are manually locked to prevent payments to individuals subject to financial sanctions or AML/CFT investigations. If a player's risk rating increases, the account remains locked until AML/CFT requirements are satisfied.

4. Risk Assessment Criteria

4.1. Understanding Risk Factors

Transactions involving virtual assets generally represent higher risk compared to fiat due to anonymity and traceability limitations. However, this alone does not categorize a customer as high risk; a combination of factors must be assessed.

4.2. High-Risk Indicators

The following indicators should be recognized as red flags or high-risk indicators during customer risk assessment:

a) Anonymiser Software and Privacy Tools

- *Red Flags*: Use of anonymiser software, mixers, or anonymity-enhanced cryptocurrencies.
- *Action*: Investigate context and purpose, assess if used to obscure funds or evade detection.

b) IP Address Discrepancies

- *Red Flags*: IP address does not match registration data.
- *Action*: Validate IP and verify identity against provided information.

c) Transaction Value Irregularities

- *Red Flags*: Transactions unusually high or low compared to typical patterns.
- *Action*: Review history and investigate reasons for fluctuations.

d) Unclear Source of Wealth

- *Red Flags*: Source of wealth cannot be verified despite reasonable effort.
- *Action*: Request additional documents or escalate for further review.

4.3. Risk Categorization

- *Low Risk*: Transparent histories, consistent IPs, verifiable wealth.
- *Medium Risk*: Occasional irregularities but generally verifiable.
- *High Risk*: One or more red flags, unclear funds, or identity concerns.

5. Risk Mitigation

5.1. Developing Treatment Plans

Strategies are developed to reduce or manage risks, including:

- Avoidance, reduction, transfer, or acceptance techniques.
- Diversification of operations and effective oversight of crypto-related risks.

6. Regulatory Compliance

6.1. Adherence to MiCA Regulation¹

- A Compliance Officer is appointed to oversee MiCA adherence.
- Updates from MiCA are reviewed and integrated into operations.

6.2. Ongoing Compliance

- The company ensures all crypto transactions comply with relevant laws and standards.
- Continuous monitoring of regulatory developments ensures alignment with evolving rules.

7. Employee Training

Employees handling crypto transactions receive ongoing training on:

- Best practices and security measures.
- Recognition of red flags and use of blockchain analysis tools.
- Awareness of regulations and compliance requirements.

8. Incident Response

A structured incident response plan includes:

- Immediate measures to limit damage.
- Comprehensive investigations and documentation.
- Regular plan updates based on new threats and vulnerabilities.

9. Review and Update

The policy is reviewed regularly to reflect changes in the crypto market, new risks, and regulatory updates. Reviews occur annually and as needed in response to emerging threats or requirements.

¹ <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>