Risk Management Policies and Procedures for Crypto Use of ENVISION DIGITAL N.V.

Objective

ENVISION DIGITAL N.V. applies blockchain-based solutions to support cashless gameplay and digital wallet operations within its online gaming platform. All cryptocurrency transactions are safeguarded by security controls and AML/CTF procedures. The company maintains a structured risk management framework to protect assets and mitigate risks linked to virtual assets.

Scope

This policy applies to all employees, departments, and affiliated entities of ENVISION DIGITAL N.V. engaged in the handling, monitoring, or processing of cryptocurrency transactions.

1. Risk-Based Approach (RBA)

1.1. Definition

ENVISION DIGITAL N.V. applies a Risk-Based Approach (RBA) to evaluate and manage risks tied to cryptocurrency use. This involves continuously identifying, assessing, and implementing measures to mitigate potential risks.

1.2. Risk Identification

Risks associated with crypto transactions are identified and recorded, including:

- market volatility,
- liquidity risk,
- cybersecurity threats,
- regulatory and compliance risks,
- operational and process-related risks.

To ensure completeness, risk identification relies on structured tools such as checklists, risk registers, and dedicated risk assessment sessions.

2. Risk Analysis

2.1. Detailed Risk Analysis

Once risks are identified, they are further analyzed by:

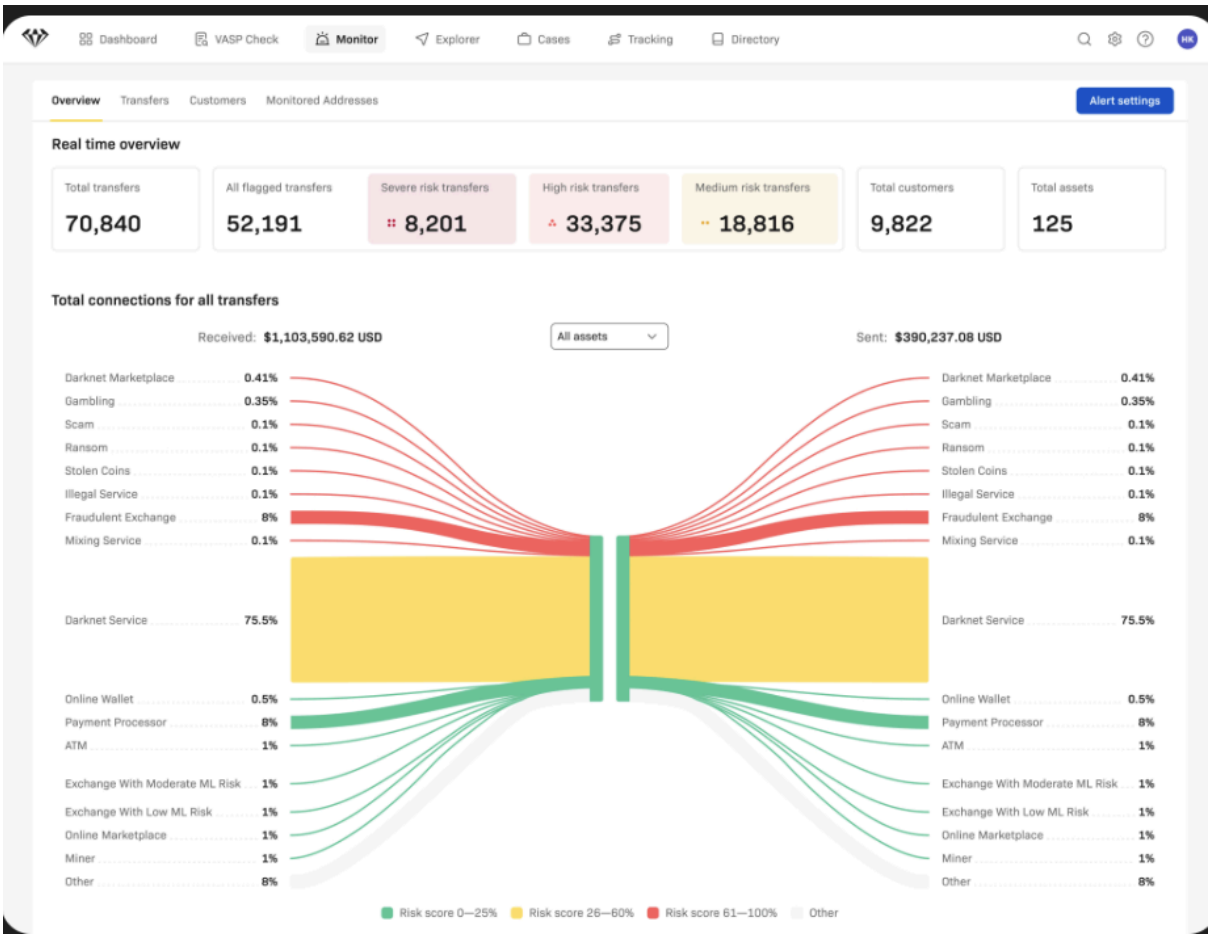
- Assessing the probability of occurrence and potential consequences.
- Applying both quantitative and qualitative methods such as scenario modeling, stress testing, and sensitivity analysis to evaluate vulnerabilities and mitigation strategies.

2.2. Transaction Monitoring

Pattern Analysis. The monitoring system observes not only the size of transactions but also player behavior: deposit frequency, gameplay activity, and irregular transaction structures. Suspicious patterns are flagged using established red-flag indicators.

Chainalysis Review. All cryptocurrency deposits and withdrawals are screened through Chainalysis to detect potential fraud or illicit activity. Accounts with alerts are suspended for investigation. High-risk players may be asked to provide proof of source of wealth. Withdrawals to wallets identified as high-risk may be refused.

Crystal Platform. Transaction monitoring is supported by the **Crystal platform**, ensuring scalable and flexible blockchain investigation tools that enable compliance with AML/CTF requirements and effective detection of financial crime.



3. Due Diligence Measures

3.1. Customer Due Diligence (CDD)

Blockchain analysis tools are used to review the origin of funds in all crypto transactions and to identify links to suspicious or fraudulent wallets.

3.2. Enhanced Due Diligence (EDD)

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

3.3. Account Blocking and Freezing

Accounts may be locked to prevent payments to sanctioned individuals or those subject to AML/CTF reviews. Accounts remain restricted until requirements are satisfied.

4. Risk Assessment Criteria

4.1. Understanding Risk Factors

Transactions involving cryptocurrencies or virtual goods carry higher inherent risks than fiat transactions due to anonymity and reduced traceability. Customers are assessed on a combination of factors rather than on a single criterion.

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 mixers, anonymiser software, or privacy-focused cryptocurrencies.
- *Action*: Investigate purpose, context, and potential attempts to obscure funds.

b) IP Address Discrepancies

- *Red Flags*: IP address does not match customer registration details.
- *Action*: Verify IP against customer-provided data.

c) Transaction Value Irregularities

- *Red Flags*: Transactions unusually large or small compared to normal patterns.
- *Action*: Review historical activity and investigate fluctuations.

d) Unclear Source of Wealth

- *Red Flags*: Wealth source cannot be validated.
- *Action*: Request additional documentation or escalate for further review.

4.3. Risk Categorization

- **Low Risk**: Consistent patterns, transparent history, verifiable funds.
- **Medium Risk**: Occasional irregularities, but generally verifiable.
- **High Risk**: Multiple red flags, attempts to conceal funds, or unverifiable sources.

5. Risk Mitigation

5.1. Developing Treatment Plans

Risk mitigation strategies are created to lower both likelihood and impact, including:

- Avoidance, reduction, transfer, or acceptance of risks.
- Portfolio diversification and proactive monitoring of cryptocurrency exposures.

6. Regulatory Compliance

6.1. Adherence to MiCA Regulation[1]

- Appointment of a Compliance Officer to oversee MiCA compliance.
- Regular integration of MiCA regulatory updates into internal procedures.

6.2. Ongoing Compliance

- Ensuring compliance of all crypto transactions with relevant legal standards.
- Continuous review of new regulations and adaptation of company policies.

7. Employee Training

Employees engaged in crypto-related operations receive ongoing training covering:

- AML/CTF standards and red-flag recognition.
- Security best practices and blockchain tool usage.

[1] https://eur-lex.europa.eu/eli/reg/2023/1114/oj

- Awareness of evolving regulations and compliance requirements.

8. Incident Response

A structured incident response framework is in place, including:

- Immediate mitigation steps,
- Comprehensive investigations,
- Documentation of incidents,
- Regular updates to reflect emerging threats.

9. Review and Update

The policy is periodically reviewed and updated to reflect market developments, new risks, and regulatory changes. Reviews are conducted annually and as required by new conditions.