

CUPWIN B.V.

**Risk Management Policies and
Procedures for Crypto Use**

Objective

We leverage advanced blockchain technology to enable cashless gaming and digital wallet systems in online casinos. We ensure that all digital wallet transactions are secure and fully compliant with AML/CTF regulations. Additionally, we employ comprehensive risk management strategies to protect assets and minimize the risks associated with using cryptocurrencies.

Scope

This policy applies to all employees, departments, and entities engaged in the use, management, and trading of cryptocurrencies.

1. Risk-Based Approach (RBA)

1.1. Definition

We adopt a Risk-Based Approach (RBA) to assess and manage risks associated with cryptocurrency use. This involves identifying, analyzing, and implementing measures to mitigate these risks effectively.

1.2. Risk Identification

We systematically identify the risks associated with cryptocurrency transactions. This includes:

- Conducting a comprehensive review of potential risks, such as market volatility, liquidity risk, cybersecurity risk, regulatory risk, and operational risk.
- Utilizing tools such as risk checklists, risk registers, and risk workshops to ensure thorough risk identification.

2. Risk Analysis

2.1. Detailed Risk Analysis

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

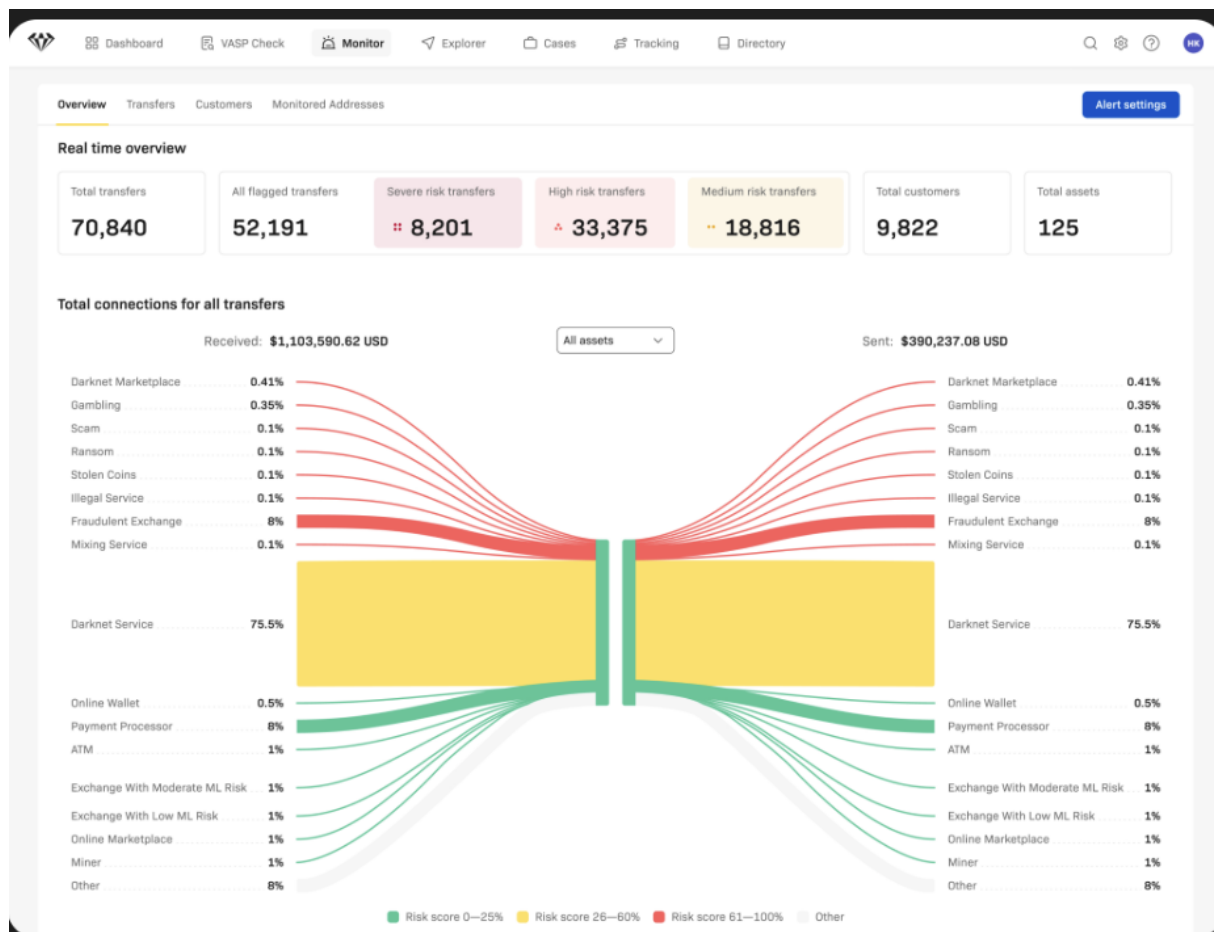
- Assessing the likelihood of each risk materializing and its potential impact.
- Employing quantitative and qualitative techniques such as scenario analysis, stress testing, and sensitivity analysis to evaluate the potential impact and effectiveness of various risk mitigation strategies.

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focuses on in-game play, deposit frequencies, and transaction patterns rather than solely on the amounts deposited or withdrawn.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.

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 transaction monitoring is provided by Crystal platform, which offers a scalable, flexible solution for crypto investigations.



3. Due Diligence Measures

3.1. Customer Due Diligence (CDD)

Blockchain Analysis Tools: We use blockchain analysis tools 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)

We conduct enhanced due diligence for high-risk clients and transactions, particularly those involving significant amounts or sources of funds that are unclear.

3.3. Account Blocking and Freezing

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

4. Risk Assessment Criteria

4.1. Understanding Risk Factors

Source of Funds: Transactions involving virtual assets or virtual goods generally represent a higher risk compared to fiat transactions due to their potential for anonymity and lack of traceability. However, this does not automatically categorize a customer as high risk. Each customer should be assessed based on a combination of factors.

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, IP mixers, coin mixers, or anonymity-enhanced cryptocurrencies.
- **Action:** Investigate the purpose and context of using these tools and assess whether they are used to obscure the source of funds or evade detection.

b) IP Address Discrepancies

- **Red Flags:** IP address does not match the registration details provided by the customer.
- **Action:** Validate the IP address and verify the customer's identity against the provided information to ensure consistency.

c) Transaction Value Irregularities

- **Red Flags:** Significant transactions involving virtual assets or virtual goods where the value is unusually high or low compared to typical transaction patterns.
- **Action:** Conduct a thorough review of transaction history and investigate the reasons for significant fluctuations in transaction values.

d) Unclear Source of Wealth

- **Red Flags:** The source of wealth is unclear or cannot be verified despite reasonable efforts.
- **Action:** Request additional documentation or evidence to clarify the source of wealth. If necessary, escalate the issue for further review (see Section 4.4 Customer Due Diligence for additional details).

4.3. Risk Categorization

- **Low Risk:** Customers with transparent transaction histories, consistent IP addresses, and verifiable sources of wealth.
- **Medium Risk:** Customers with occasional high-value transactions or minor discrepancies in IP addresses, but who otherwise provide verifiable information.
- **High Risk:** Customers exhibiting one or more red flags, such as using anonymizer tools, significant transaction value discrepancies, or unclear sources of wealth.

5. Risk Mitigation

5.1. Developing Treatment Plans

We develop comprehensive risk mitigation strategies to minimize the likelihood and impact of identified risks by:

- Implementing risk avoidance, risk reduction, risk transfer, and risk acceptance techniques.
- Ensuring appropriate portfolio diversification and effective management of risks associated with cryptocurrency use.

6. Regulatory Compliance

6.1. Adherence to MiCA Regulation¹

- Compliance Officer: Appoint a Compliance Officer to oversee adherence to MiCA regulations.
- Regulatory Updates: Review and integrate updates from MiCA into existing practices regularly.

6.2. We ensure all cryptocurrency transactions comply with relevant regulations and standards by:

- Staying updated on legal changes and adjusting our policies accordingly.
- Continuously monitoring regulatory developments to maintain compliance.

7. Employee Training

We provide regular and comprehensive training to our employees on cryptocurrency use and associated risks, which includes:

- Educating employees on best practices and security measures.
- Enhancing skills through recorded interactions and ongoing education.
- Ensuring awareness of the latest regulations and compliance requirements.

8. Incident Response

We have established a clear incident response plan to address potential security breaches or losses by:

- Taking immediate action to mitigate damage.
- Conducting thorough investigations and documenting incidents.
- Regularly updating and improving the response plan based on new threats and vulnerabilities.

9. Review and Update

We regularly review and update our risk management policies to reflect changes in the cryptocurrency market and emerging threats. This involves:

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

- Continuously monitoring risk factors.
- Adapting to new regulations and technological advancements.
- Conducting annual reviews and making necessary adjustments.