

Green Forest Group N.V.
Business Risk Assessment
(BRA)

Table of Contents

1.	Overview and Objective	3
2.	Responsibilities	3
3.	Risk Assessment	3
4.	Criteria Risk Assessment	4
5.	Process – Risk Assessment	5
6.	Evaluation and Analysis of Risks.....	5
7.	Effectiveness.....	6
8.	Risk Identification, Analyses and Evaluation	7
9.	AML/CFT Risk Management Process	8

1. Overview and Objective

Green Forest Group N.V. (hereinafter referred to as "the Company") has established comprehensive measures to effectively mitigate the risks associated with Money Laundering and the Financing of Terrorism (ML/FT).

The Company operates within the regulatory framework set forth by the Curacao Gambling Authority (CGA) and holds a Business-to-Consumer (B2C) license, which authorizes it to provide remote gaming services to eligible clients. Its core mission is to offer gaming entertainment across jurisdictions deemed acceptable by the Curacao Gaming Control Board (GCB), fully compliant with applicable terms, conditions, and regulatory standards.

Operating under the brand name www.epybet.com, the Company utilizes its proprietary gaming platform to deliver its services, ensuring operational functionality across all critical sectors, including player registration, transaction processing, customer support, and responsible gaming practices.

In strict adherence to its obligations as a subject person under Curacao's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regulations, the Company has undertaken a comprehensive AML/CFT Business Risk Assessment (BRA) to identify, assess, and manage the risks associated with its activities and service offerings.

Aligned with its overarching risk management framework, the Company has adopted and maintains a Medium Risk Appetite, balancing its commitment to business growth with the need to proactively address and minimize exposure to ML/FT threats.

2. Responsibilities

The Compliance Officer bears primary responsibility for the supervision and monitoring of all customer transactions and the verification of the identities of registered players. Beyond these core duties, the Compliance Officer is also responsible for establishing clear and effective criteria for the early detection of potentially suspicious activities. They must design, implement, and continuously update internal protocols to address identified risks and ensure that exposure to Money Laundering and Financing of Terrorism (ML/FT) threats is minimized to the greatest extent possible.

However, the obligation to combat ML/FT is not limited to the Compliance Officer alone. Every employee of the Company who is involved in customer-facing operations, payment processing, or transaction monitoring must actively participate in the Company's overarching Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) framework. This includes strict adherence to the Company's established policies, operational procedures, and internal controls designed to detect and prevent illicit activities.

To support this collective responsibility, the Company must ensure that all relevant employees receive comprehensive and ongoing AML/CFT training programs. These training sessions are designed not only to enhance awareness of emerging ML/FT risks but also to reinforce employees' understanding of their personal and professional obligations under the regulatory regime. Training must be updated regularly to incorporate changes in legislation, regulatory guidance, and identified risk trends.

3. Risk Assessment

Risk is defined as the possibility of an adverse event occurring, or the failure to achieve a desired outcome, which negatively impacts business operations, reputation, or financial stability. Risks become evident in a variety of situations, including:

- Failure to meet established business objectives and performance targets.
- Non-compliance with internal organizational policies, external regulations, or relevant legislation.
- Inefficient, ineffective, or inappropriate use of business resources or assets.

To proactively manage these risks, the Company must implement a comprehensive and effective risk assessment and management framework. This framework should be designed not only to prevent potential threats from arising but also to ensure that contingency plans are in place to mitigate the impact of risks if they do materialize.

The risk management process should be robust, standardized, and well-documented, providing clear guidelines for conducting assessments. This ensures that assessments produce consistent, valid, and comparable results, regardless of who conducts them or when they are carried out.

In line with industry standards, the Company adheres to risk assessments performed by the Curacao regulatory authorities, as well as relevant supranational risk assessments for the gaming sector. These assessments consistently highlight the gaming industry as a high-risk environment due to its susceptibility to various forms of financial crime, including money laundering and terrorist financing. The Company also aligns its operations with the Curacao Framework, ensuring that its risk management processes are in line with national and international best practices.

4. Criteria Risk Assessment

There are various situations in which conducting an Anti-Money Laundering and Financing of Terrorism (AML/CFT) risk assessment becomes essential for the Company. These situations typically include:

- Performing a comprehensive risk assessment that evaluates a wide range of factors, including the diverse customer types the Company serves, the range of services it provides, the communication channels used to interact with customers, and the geographical regions in which the Company operates. This ensures a holistic understanding of the associated risks.
- Integrating periodic updates to the AML/CFT risk assessment into the Company's regular management review process. This ongoing review helps to adapt to changing internal and external conditions, ensuring the Company remains vigilant to emerging risks.
- Evaluating internal projects or strategic initiatives that are expected to introduce significant changes to the Company's business model. These changes may involve new services, markets, or technological innovations, each of which could introduce new risks that require thorough assessment.
- Undertaking a reassessment of the existing risk landscape when substantial external events or changes occur that could render prior risk assessments outdated or incomplete. Such events include alterations to applicable laws, regulations, or other significant shifts in the external environment that could affect the Company's risk exposure.

In cases where there is any doubt or ambiguity regarding whether a risk assessment is needed, the Company should adopt a precautionary approach and proceed with conducting an assessment. This ensures that potential risks are proactively identified and addressed, minimizing the possibility of compliance gaps.

5. Process – Risk Assessment

The risk assessment process follows a structured series of steps as outlined below:

- **Asset Identification:** This step involves recognizing the critical assets at risk related to Anti-Money Laundering and Financing of Terrorism (AML/CFT). The primary focus is on protecting assets such as the Company's reputation and its compliance standing. Failure to safeguard these assets could lead to severe consequences, including the suspension of operational licenses, financial penalties, or potential legal action against individuals responsible for AML breaches.
- **Risk Area Identification:** This step is concerned with identifying the various risk areas across the organization. It encompasses customer types, services provided, communication channels used, geographical locations of operation, as well as both internal and external operational risks, particularly those related to employees who manage customer relationships.
- **Threat Identification:** This involves evaluating threats specific to each identified risk area, taking into account known occurrences and vulnerabilities within the Remote Gaming Industry. Understanding these threats allows the Company to anticipate and prepare for potential risks.
- **Vulnerability Assessment:** Here, the Company assesses vulnerabilities that arise from factors such as limited face-to-face interactions with customers, the use of diverse payment methods, and the potential inadequacies in AML/CFT frameworks in certain jurisdictions. These vulnerabilities are critical to understanding areas where the Company is more susceptible to risk.
- **Risk Scenario Identification:** This step identifies specific risks to compliance and business operations through collaborative discussions and interviews with relevant stakeholders. The findings are documented in a Risk Matrix, which includes feedback from the Director of Green Forest, the Compliance Officer, and employees engaged in customer relations and payment processing.
- **Probability Assessment:** In this step, the likelihood of identified threats materializing is estimated based on historical data, trends within similar organizations, and the presence of sufficient motive, opportunity, and capability for the threat to manifest. This assessment is vital to gauge the likelihood of a risk occurring in the future.
- **Impact Assessment:** Finally, the Company evaluates the potential consequences of Money Laundering and Financing of Terrorism incidents. This includes assessing the legal, compliance, and operational impacts on the Company, as well as the broader implications for individuals and countries potentially vulnerable to terrorist activities.

This structured process ensures that all aspects of AML/CFT risk are thoroughly assessed, with an emphasis on proactive identification, evaluation, and mitigation of risks.

6. Evaluation and Analysis of Risks

To assess risks to assets and develop appropriate mitigation strategies, the Company has conducted a comprehensive analysis covering potential threats, vulnerabilities, the likelihood of occurrences, and the possible impact of such events. A 5-point scale is employed to quantify both the probability of risk and its corresponding impact.

The likelihood scale ranges from 1 (improbable) to 5 (almost certain), while the impact scale spans from 1 (negligible) to 5 (very high). This organized method enables effective risk prioritization, aiding in the development of more targeted management strategies. The risk matrix shown below visually displays these scales and supports the prioritization of risks.

The classification of each risk is based on the score derived from multiplying the likelihood and impact ratings. With both scales ranging from 1 to 5, the final scores range from a minimum of 1 to a maximum of 25, as shown in the matrix. Risks are categorized as follows:

- High: Scores of 12 or higher
- Medium: Scores between 5 and 10
- Low: Scores from 1 to 4

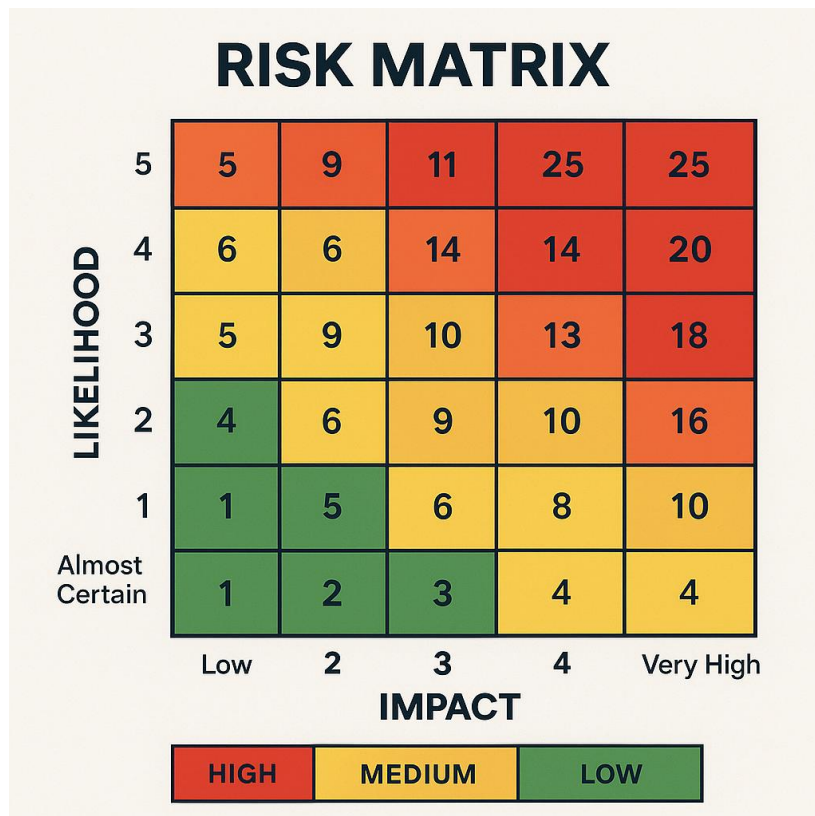


Figure 1 Risk Matrix Table Sample

The reasoning behind the assigned likelihood and impact ratings is documented to ensure that any significant changes can be assessed over time. If any material changes occur, the risk matrix will be updated, maintaining consistency in the evaluation of risks.

7. Effectiveness

The table below demonstrates the performance of the applied controls, offering a clear view of their strength in mitigating identified threats. This evaluation supports the analysis of the remaining (residual) risk level after all risk-reduction measures have been executed.

Mitigation Level	Description
4 – Robust	Controls are comprehensive, consistently applied, and proven to effectively mitigate associated risks. No immediate improvements are necessary.
3 – Adequate	Controls are generally effective and applied with reasonable consistency. Risk is managed satisfactorily, though some enhancements could improve overall performance.

2 – Limited	Controls exist but are inconsistently applied or only partially mitigate risk. Significant improvements are required to manage threats effectively.
1 – Absent	No meaningful controls are in place, or existing measures fail to mitigate the risk. Immediate corrective action is required.

The diagram below provides a structured representation of the methodology used to determine the Residual Risk outcome. This process involves evaluating the level of inherent risk, defined as the exposure to risk in the absence of any controls—and assessing the effectiveness of the existing mitigation measures. By cross-referencing these two variables in a matrix, the residual risk level is calculated. This outcome reflects the degree of risk that remains after all mitigating controls have been applied, and serves as a key indicator for decision-making in risk management strategies.

Residual Risk				
		Inherent Risk		
		Low	Medium	High
Aduacus Adequacy	Robust	Low	Low	Medium
	Adequate	Low	Medium	Medium
	Limited	Medium	Medium	High
	Absent	Medium	High	High

Figure 2 Residual Risk

8. Risk Identification, Analyses and Evaluation

The following table presents an overview of the key business risk factors related to money laundering and terrorist financing (ML/FT), including the primary threats identified and the corresponding mitigation measures established.

A comprehensive breakdown of the risk identification and analysis process—along with an evaluation of the effectiveness of the controls, internal policies, procedures, and other risk mitigation strategies currently in place at Green Forest Group N.V.—can be found in the accompanying document titled "Green Forest Group Risk Assessment Matrix – V1.0."

Risk Factor	Risks Identified	Mitigation Measures Implemented	Residual Risk
Interface	- Lack of in-person interactions increases the risk of customer anonymity and identity fraud.- Potential for misuse of digital onboarding channels.	- Customer Due Diligence (CDD) conducted at onboarding and upon reaching transactional thresholds.- Enhanced monitoring of behavioural patterns and unusual activity.	Medium
Customer	- Diverse customer types including PEPs, VIPs, and high-risk individuals.- Risk of fraudulent or multiple account registrations.	- Standard and Enhanced Due Diligence applied based on risk classification.- Targeted screening of VIPs and PEPs using reliable databases.- Continuous transaction monitoring.	Low
Product	- Abuse of certain products or payment functionalities (e.g., prepaid cards, rapid withdrawals).- Exploitation through repetitive behaviour patterns.	- Real-time monitoring of transactions for anomalies.- Implementation of strict controls on deposits and withdrawals.- Reporting of suspicious transactions as required.	High
Geographical	- Customers accessing services from jurisdictions listed as high-risk by FATF or similar bodies.- Use of payment methods linked to high-risk territories.	- Routine Geographical Risk Analysis mapped against FATF lists.- Application of SDD, CDD, and EDD as per risk level.- Regular review of country risk indicators.	Medium
Employee Risk	- Possibility of unintentionally or intentionally facilitating ML/FT due to lack of awareness or controls.- Assignment of AML responsibilities inappropriately.	- Thorough pre-employment screening of relevant staff.- Mandatory AML/CTF training and regular refreshers.- Supervision and periodic internal audits.	Medium
Outsourcing	- AML obligations are performed in-house; outsourcing such functions is restricted or non-permissible under the company policy.	- Not applicable, as AML tasks are exclusively managed internally under strict oversight.	N/A

9. AML/CFT Risk Management Process

The overall medium risk rating assigned to all identified risk factors is deemed reliable only if Green Forest Group N.V. constantly and effectively enforces its Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), Fraud Prevention, Business, and Customer Risk Management

Policies and Procedures. The ongoing success of this risk level classification is also contingent upon the company's continuous monitoring and scrutiny of customer activity across all operational channels.

As part of this assessment, the company's relevant internal policies and procedures have been thoroughly reviewed and updated to reflect the current AML/CFT Risk landscape. These updates are essential to ensure that the control framework remains effective and proportionate to the level of risk identified.

The company is committed to conducting periodic reviews and timely updates of these procedures, with the objective of maintaining full alignment with applicable legal and regulatory obligations. Moreover, regular evaluations of the adequacy and efficiency of implemented risk mitigation measures will be performed to ensure that the residual risk remains within acceptable limits, as defined by the company's stated risk appetite.

This AML/CFT Risk Assessment shall be reviewed and updated at least once every 12 months. However, it must also be re-evaluated sooner if there are any significant changes in the company's operational structure, customer base, product offering, risk exposure, or applicable laws and regulations.

Until the next scheduled review date, the company must maintain heightened awareness of any developments that could impact its risk profile. Any such changes may trigger an early reassessment of this document to ensure continued relevance and regulatory compliance.

Current Risk Evaluation Summary:

Inherent Risk Level: Medium

Residual Risk Level: Medium