

Alisium B.V.

(Reg. number 161507)

**Business Risk Assessment Methodology
and Documentation Standards**

Contents

1. Version Control	3
2. Abbreviations and Definitions	4
3. Introduction	5
4. Business Risk Assessment Purpose	5
5. Risk Governance	5
6. Business Risk Assessment Methodology	5
7. The Risk Assessment Process Flow include:	6
7.1 Identification of Assets	6
7.2 Identification of Risk Areas	6
7.3 Identification of Potential Threats and Vulnerabilities	7
7.4 Risk Scenarios Identification	8
7.5 Likelihood assessment	8
7.6 Impact Assessment	8
8. Risk factors	8
8.1 Geographical Risk	8
8.2 The Customer Risk	8
8.3 Product/Service/Transaction Risk	9
8.4 Interface/ Delivery Channel Risk	9
8.5 Internal Risk	9
8.6 Technology Risk	9
9. Numerical Classification	9
10. Results of national and supranational risk assessment	11
11. Business Risk Assessment Revision	11

1. Version Control

Name	Description
Document Name	Business Risk Assessment Methodology and Documentation Standards
Version	1.3
Author	Compliance Department
Authorised By	The Board of Directors
Last Approval Date	
Last Review Date	

Version	Description / Changes	Date
1.0	Implementation	15.05.2023
1.1	Document review and update	01.05.2024
1.2	Document review and update	20.03.2025
1.3	Document review	12.12.2025

2. Abbreviations and Definitions

ML/TF / PF - Money Laundering / Terrorism Financing / Proliferation of Weapons of Mass Destruction

AML – Anti-Money Laundering

BRA – Business Risk Assessment

CDD – Customer Due Diligence

CPF - Countering Proliferation of Weapons of Mass Destruction

CTF – Combating the Terrorism Financing

CGA – Curacao Gaming Authority

The Company – means a Curacao registered company, Alisium B.V., reg. Number 161507

Client – A natural person, who has a business relationship with and uses the services provided by the Company, based on the concluded servicing agreement (Terms of Use).

Employee – An Employee, who is engaged in fulfillment of AML responsibilities, conducts CDD/EDD procedures, analyses the relevant information pertaining to the Client, performs risk assessment of the Client and performs other functions, as may be required to fulfill the Company's AML/CTF obligations.

3. Introduction

Alisium B.V. ('the Company') is a Curacao Company offering remote betting and gambling services under the Business to Customer License OGL/2024/227/0112.

4. Business Risk Assessment Purpose

The purpose of this document is to assess the ML/TF/PF risks the Company is exposed to and to apply appropriate measures and controls to mitigate those risks.

By implementing a risk management plan and considering the various potential risks or events before they occur, the Company can save money and protect its future. This is because a robust risk management plan shall help the Company establish procedures to avoid potential threats, minimize their impact should they occur and cope with the results. This ability to understand and control risk enables the Company to be more confident in its business decisions. Furthermore, strong corporate governance principles that focus specifically on risk management can help the Company reach its goals.

Other important benefits of risk management include:

- ☐ Creates a safe and secure work environment for all staff and Clients;
- ☐ Increases the stability of business operations while also decreasing legal liability;
- ☐ Provides protection from events that are detrimental to both the Company and the environment;
- ☐ Protects all involved people and assets from potential harm.

5. Risk Governance

The Company places significant importance on the provision of relevant and timely risk information across all levels within the Company in order to promote effective risk management throughout the Company. Responsibility for risk management resides at all levels within the Company from the Board of Directors down through the Company. The Company applies risk management responsibility distribution so that risk-return decisions are taken at the most appropriate level.

6. Business Risk Assessment Methodology

The Company has adopted a methodology as recommended by FATF that sets out how to assess the likelihood and impact of identified risks and how to assess the effectiveness of the respective controls. As detailed below the methodology includes:

- ☐ Identifying the inherent risk by carrying out risk assessment and assessing the impact and likelihood of the risk on the business
- ☐ Assessing and then applying controls by mitigation, managing, and monitoring and periodic reviews

- ☐ Assessing the effectiveness of the Company controls and
- ☐ Achieving a residual risk that is acceptable by the Company.

Risk management of the Company is adapted to the business objectives and is based on the principles described below:

- ☐ Collective responsibility for risk, but also individual accountability
- ☐ Full representation on risk matters at the Board level
- ☐ Integration of risk management within all business functions

7. The Risk Assessment Process Flow include:

1. Identifying assets
2. Identifying Risk Areas
3. Identifying potential Threats
4. Identifying Vulnerabilities
5. Risk scenario identification
6. Assess likelihood
7. Assess impact

7.1 Identification of Assets

The internal asset at risk in the context of AML/CTF/CPF is the reputational asset with both the customers and public as well as the Company's reputation with the regulators. The compliance status of the Company which if not protected could lead to potential suspension of a license to operate, administrative fines and/or potential criminal prosecution for the persons entrusted to prevent the occurrence of ML/TF/PF through the Company's business.

The Company must also ensure that it protects its reputation from adverse media coverage, and/or, even worse, regulatory action may seriously jeopardize the trust enjoyed by the Company's customers.

7.2 Identification of Risk Areas

The remote gaming licensees are expected to consider risk factors when drawing up their business risk assessment. These are the risk factors that are specific to the remote gaming sector and the Company has considered and assessed them in relation to its customer base.

Figure 1 lists the risk factors that the company is exposed to prior to application of control measures, i.e., inherent risks and after suitable controls have been put in place i.e., residual risks.

Figures 2, 3, and 4 of Section 9 “Numerical Classification” explains how the following Level of Risks were identified.

Risk Factors	Inherent Risk Level	Range of Residual Risk Levels
Customer Risks	Low	Low
Interface Risk	Low	Low
Geographical risks	Low	Low
Service, Product Transaction risks	Low	Low
Internal risks	Low	Low
Technology risks	Low	Low
Resulting risk evaluation	Low	Low

Figure 1 Risk Factors

In addition to the risk factors listed the Company has taken into consideration the Curacao NRA 2020¹, which lists the gaming sector ML/TF vulnerabilities. It is the controls within its own AML/CFT/CPF framework that the Company has adopted to mitigate the identified inherent risks. The more detailed description is outlined in “Results of national and Supranational risk assessments” in the following pages of this document. The Company acknowledges that it is the maintenance of the residual risk level and the potential reduction to a lower risk level is dependent on the proper and consistent application of its policies and procedures and controls.

7.3 Identification of Potential Threats and Vulnerabilities

The assessment process has identified risks related to customer types, remote gaming services offered (products), payment methods (transactions), geographical risks, customer financial activity risks and technology risks. The process has also considered internal risks related to the employees involved in managing the Company’s customer relationships and financial activity as well as the tools available for better monitoring and management of the relevant risks. The potential threats of ML/TF/PF occurring in each risk area have been assessed based on threats that are known to occur within the remote gaming industry. These threats are known to derive mainly from vulnerabilities of non-face-to-face relationships such as identity theft, fraudulent transactions, as well as threats arising from cash-based transactions and terrorist groups.

These and other vulnerabilities were assessed and identified to be arising from:

- ☐ Nature of a non-face-to-face customer relationships;
- ☐ Geographic offering of services across different countries;

¹ <https://minfin.cw/wp-content/uploads/2023/05/Publieke-Versie-NRA-Curacao-2020.pdf>

- ☐ Exposure to different types of payment instruments;
- ☐ Gaming products accessed through remote means;
- ☐ Lack of adequate automation and/or manual processes or failures where present; and,

The identification of ML/TF/PF threats and vulnerabilities has been achieved by:

- ☐ Using a combination of brainstorming and discussions between the involved teams' management Employees;
- ☐ Referring to open sources and regulatory guidance for assessing geographical risk and payment method risk.

7.4 Risk Scenarios Identification

The identification of risks to compliance and business activities has been performed by a combination of group discussions and interviews with the interested parties.

7.5 Likelihood assessment

An estimate of the likelihood of a threat occurring has been carried out. This estimation has taken into consideration whether an event has occurred before, either to our Company or similar organizations in the same industry, and whether there exists enough motive, opportunity, and capability for the threat to materialize.

7.6 Impact Assessment

An assessment of the impact that incidents of Money Laundering, Funding of Terrorism, Proliferation of Weapons of Mass Destruction can have on the business and on society in general have been considered.

Consideration has been given to the multiple areas mentioned, but it is not being quantified in monetary value as such calculations are deemed to be outside the scope and objectives of this risk assessment. AML/CTF/CPF compliance risks cannot be disregarded or reduced to a simple monetary value due to their knock-on effect on the Company and the well-being of the public as well as the reputation of the licensing Authorities.

8. Risk factors

8.1 Geographical Risk

The Geographical risk can be defined as additional risk arising from differences in economic, political, and legal environment, when operating internationally or cross-border. The geographical risk is posed to the Company by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship.

8.2 The Customer Risk

The risk of ML/TF/PF may vary in accordance with the type of customer. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth.

8.3 Product/Service/Transaction Risk

Some products/services/transactions are inherently riskier than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services

8.4 Interface/ Delivery Channel Risk

The channels through which the Company establishes a business relationship and/ or through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. Channels that favor anonymity increase the risk of ML/TF/PF if no measures are taken to address the risk.

8.5 Internal Risk

The internal Risk can be defined as additional risk arising from employees being not suitable for the position where they perform AML/CTF/CPF duties, lack of knowledge and from employees intentionally and/or unintentionally not observing controls to allow ML/TF/PF.

8.6 Technology Risk

The risks of misuse of technological developments for the purpose of money laundering, the financing of terrorism or proliferation of weapons of mass destruction.

9. Numerical Classification

To assess the risk to an asset and determine the appropriate treatment, the Company has examined the threats, vulnerabilities, the likelihood that the threat will take place and the impact of it should it occur. A 5-point scale has been used to describe the likelihood of a risk occurring and to describe the impact that it is likely to have.

The 5-point scale for the likelihood ranges from 1=improbable to 5=almost certain; the 5-point scale for the impact ranges from 1=negligible to 5=very high. The risk matrix shown below illustrates the scales and allows the Company to prioritize risks so that they can be managed more effectively.

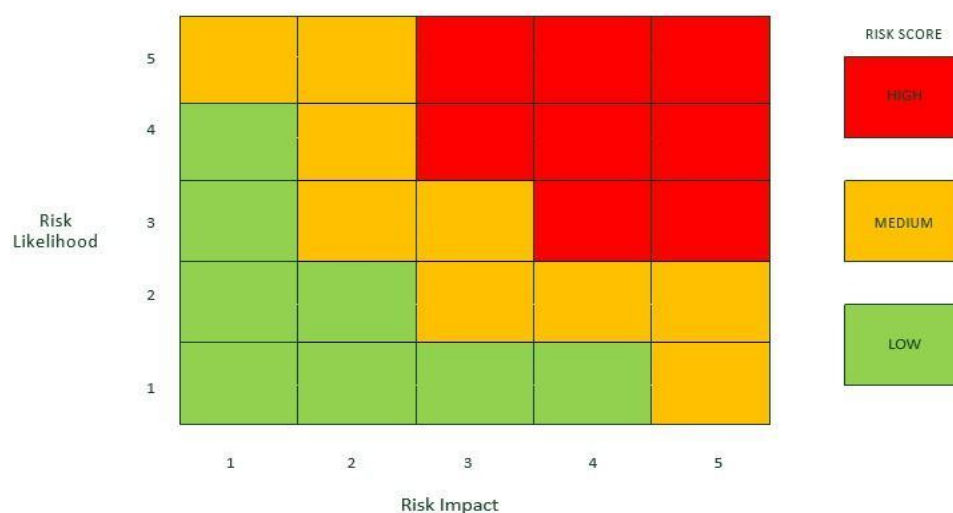


Figure 2 – Risk Matrix Chart

The risk classification considered is the score obtained from multiplying the likelihood that the risk will occur by the impact it is likely to have. Both scales range from 1 to 5, so the minimum score will be 1 and the maximum score will be 25 as shown in the matrix above.

Each risk has been allocated a classification based on its score as follows:

HIGH	12 or more
MED	5 to 11 inclusive
LOW	1 to 4 inclusive

The rationale for indicating the likelihood and impact ratings allocated has been given so that these can be assessed in the future to see if they have materially changed. This will also assist in ensuring consistency and repeatability in risk assessments.

An effectiveness score is used to ascertain how effective the measures are at mitigating the inherent risk. Consideration of the inherent risk level considering the effectiveness score assists the Company in determining the residual score. Figure 3 describes the level of effectiveness of controls in place.

Level of Mitigation	Description of Effectiveness
4 – Strong	There are measures in place to control risk that are fully operational and fully effective
3 – Effective	Risk is managed adequately but could be improved in certain parts – mitigating measures work adequately and are effective
2 – Ineffective	Risk is not managed adequately, substantial improvement necessary but has some effect
1 – Non-Existent	No controls or controls are ineffective

Figure 3 Effectiveness of the controls

Outcome of Residual Risk through the Effectiveness of the Measures in place

Effectiveness of controls	Inherent Risk			
		Low	Medium	High
	Strong	Low	Low	Medium

	Effective	Low	Medium	Medium
	Ineffective	Medium	Medium	High
	Non - Existent	Medium	High	High

Figure 4

10. Results of national and supranational risk assessment

While identifying and assessing the ML/TF/PF risks the Company is exposed to, the national and industry-specific risk assessments have been taken into consideration.

According to the European Commission Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities² the non-financial sector is increasingly attracting the attention of would-be money launderers. The report also specifies that the online gambling industry has a high risk exposure due to very large numbers of transaction- flows and the lack of face-to-face interaction..

As already mentioned in the National and Supranational Risk assessments the provision of services and the carrying out of occasional transactions on a non-face-to-face basis increases the risk of ML/TF/PF and customer impersonation. This is due to a number of factors, such as the ease of accessing services at any time and from any location, the possibility of setting up multiple fictitious accounts and avoiding detection, the absence of physical documents that can be viewed and the speed with which services are provided and transactions carried out.

The Company's exposure to the above-named risks and other risks identified in the latest national and supranational risk assessments were duly taken into consideration.

11. Business Risk Assessment Revision

The Company's business risk assessment has to be revised whenever there are changes to the external environment within which the Company is operating, such as regulatory changes and developments in technologies creating new threats and changes within its business structures/activities. Thus, situations such as a widening of the customer-base or the addition of games and payment methods which present a different risk profile from those already offered shall lead to a revision of the business risk assessment. The same shall apply when the Company changes its structure or undertakes major operational changes. In the absence of any of the above, The Company shall assess its business risk assessment at least once a year, to evaluate whether any changes thereto are necessary.

² <https://op.europa.eu/en/publication-detail/-/publication/0b2ecb04-aef4-11e9-9d01-01aa75ed71a1/language-en>
https://ec.europa.eu/info/sites/default/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf