

Temple Holdings N.V.

Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) Policy

CONFIDENTIALITY STATEMENT

This is a confidential document for Temple Holdings N.V. It contains confidential and/or proprietary information that may not be disclosed or discussed with anyone outside the organization without written approval of Temple Holdings N.V.

Disclaimer

NO PART OF THIS DOCUMENT MAY BE REPRODUCED, TRANSMITTED OR IN ANY OTHER WAY DISTRIBUTED WITHOUT THE PRIOR WRITTEN PERMISSION OF TEMPLE HOLDINGS N.V. ALL TECHNOLOGIES, DESIGNS, IMPLEMENTATIONS, TRADE SECRETS AND BUSINESS MODELS DESCRIBED HEREIN IS THE INTELLECTUAL PROPERTY OF TEMPLE HOLDINGS N.V. AND/OR IT'S PARTNERS AND IS PROVIDED FOR INFORMATION PURPOSES ONLY.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY CONCERNING ITS ACCURACY OR QUALITY. IN NO EVENT WILL TEMPLE HOLDINGS N.V. BE LIABLE FOR DIRECT OR INDIRECT DAMAGES RESULTING FROM INCIDENTAL DEFECTS OR INACCURACIES IN THIS DOCUMENT.

TEMPLE HOLDINGS N.V. RESERVE THE RIGHT TO REVIEW AND MODIFY DIGITAL COPIES OF THIS DOCUMENT AT ANY TIME WITHOUT PRIOR NOTICE.

THE TEMPLE HOLDINGS N.V. NAMES, THE TEMPLE HOLDINGS N.V. LOGOTYPES, GAME BRANDS, SERVICES AND PRODUCT NAMES ARE REGISTERED TRADEMARKS AND/OR SERVICE MARKS OF TEMPLE HOLDINGS N.V.

Contact

Temple Holdings N.V.
Mark Cauchi
+356 2166 0939
support@betkudos.com

Initial


DS


Document Version Control

Temple Holdings N.V. – AML/CTF Policy	
VERSION CONTROL	
Current version	1.1
Effective Date	2025-05-16
Sign Off Date	2025-05-16
Document Owner	Senior AML/CFT Compliance Officer
Next Review Date	2026-05-15
Comments	The policy will be reviewed on the following basis: No less than once annually, with such review to be initiated by the Policy owner approximately one month prior to the date following 12 months from which the procedure was last approved. · In response to any changes in relevant regulation and/ or legislation. · In response to general guidance notes or best practice guidance issued by any relevant regulator. · In response to any regulatory action taken · In response to findings of a relevant internal or external audit; or · Upon request of management.
Purpose	Amendments to reflect regulatory requirements according to the AML Policy template guidelines

Version history

Version	Date	Author	Purpose
1.0	2024-08-23	Temple Holdings N.V.	Creation of this AML/CTF Policy
1.1	2025-05-16	Temple Holdings N.V.	Yearly review and amendments to reflect regulatory requirements according to the AML Policy template guidelines published by the CGA

Initial


DS


Table of Contents

1. Introduction & Background	7
1.1 Scope & Purpose	7
1.2 Definitions	7
1.2.1 Money Laundering	7
1.2.2 Terrorist financing	7
1.2.3 Financing of Proliferation of weapons	7
1.2.4 Targeted Financial Sanctions	8
1.3 Definition of “Client” and “Applicant for Business”	8
1.4 Audience	8
1.5 Law, Regulations and Rules	9
1.6 Document Structure	9
1.7 Consequences of non-compliance	9
2. AML Systems and Controls – General	10
2.1 Provisions from the Nois and the Norut	10
2.2 Policy	11
2.3 Procedures and documentation	12
3 Risk Assessment, Management and Risk-Based Approach	13
3.1 Provisions of the NOIS	13
3.2 Guidance on Implementation	13
3.3 Policy	14
3.4 Procedures & Documentation	15
4. Customer Due Diligence	17
4.1 Guidance from CGA Regulations	17
4.2 Guidance on implementation	17
4.3 Policy	18
4.4 Procedures and Documentation	18
5. Ongoing monitoring	19
5.1 Provisions from the Regulations	19
5.1.1 Ongoing monitoring of identity	19
5.1.2 Ongoing monitoring of transactions	19
5.2 Guidance on Implementation	19
5.3 Policy	20
5.4 Procedures and Documentation	20
6 Reporting	21
6.1 Provisions from the CGA’s AML regulation	21
6.2 Guidance on Implementation	21
6.3 Policy	22

Initial
MC

DS
[Signature]

6.4	Procedures and Documentation	23
7	Record-Keeping Procedures	24
7.1	Provisions from the NOIS and the NORUT.....	24
7.2	Guidance on Implementation.....	25
7.3	Policy.....	25
7.4	Procedures & Documentation	25
8.	Awareness and Training.....	26
8.1	Provisions from the NOIS.....	26
8.2	Guidance on Implementation.....	26
8.3	Policy.....	27
8.4	Procedures & Documentation	28
8.5	Anti-Bribery & Corruption Policy	29
9.	The screening process.....	30
10.	Sanctions Lists	31
10.1	Guidance on Implementation.....	31
10.2	Policy.....	31
10.3	Procedures and Documentation	31
11.	Politically Exposed Persons.....	32
11.1	Provisions from the NOIS.....	32
11.2	Guidance on Implementation	32
11.3	Policy.....	32
11.4	Procedures and Documentation	32
Annex I – AML/CFT Compliance Officer Job Description.....		33
Annex II – Risk Mitigation Matrix and Risk Factors		35
Risk Assessment and Mitigation Matrix		35
Risk Factors Table.....		38
Process for Determining Customer Risk (to be implemented)		39
Annex III – Customer Due Diligence.....		39
Persons subject to Identification and Verification.....		39
Organogram		40
Due Diligence for Natural Persons		40
Due Diligence for Legal Persons.....		42
Part A.....		42
Part B.....		43
Part C.....		43
Languages		44
Client Terms and Conditions		44
Customer Risk Assessment		44

Initial
MC

DS
✓

Face-To-Face Transactions or Clients 44

Timing of Due Diligence 45

Annex IV – Client Acceptance Policy 46

Client Acceptance..... 46

Excluded Activities..... 46

Excluded Individuals 46

Risk-Based Approach for Accepting Clients 46

Annex V – Internal UTR Form 47

Annex VI – Business Risk Assessment 50

Annex VII – Abbreviations..... 51

Annex VIII – Signatory page 52

Initial


DS


1. Introduction & Background

1.1 Scope & Purpose

The provisions in this Anti-Money Laundering Policy (this “Policy”) aim to reduce the possibility for the business of providing services by Temple Holdings N.V. to be used for criminal purposes or in violation of regulations.

Temple Holdings N.V. is a Curaçao licensed online gaming entity. Mammillaria Investments Limited is a subsidiary and payment processing company on behalf of Temple Holdings N.V. only.

Being a remote gaming entity authorized under Curaçao jurisdiction, Temple Holdings N.V. is deemed to be carrying out “relevant financial business” in terms of the CGA’s AML/CFT/CFP Regulations and thus Temple Holdings N.V. is a subject-person in terms of said Regulations. As such, it is required to abide by the applicable legislation and guidance relating to the prevention of money laundering and funding of terrorism.

This Policy provides guidance detailing responsibility regarding the prevention of money laundering and funding of terrorism from the perspective of the legal framework of Curaçao and internationally accepted regulations in this area. This information includes due diligence, monitoring, training and record-keeping policies and procedures, as well as a description of the role and responsibilities of the Compliance Officer.

1.2 Definitions

1.2.1 Money Laundering

“Money laundering” means:

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- Placement;
- Layering; and
- Integration.

1.2.2 Terrorist financing

“Terrorist financing” or “Financing of Terrorism” means:

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

1.2.3 Financing of Proliferation of weapons

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

Initial


DS


1.2.4 Targeted Financial Sanctions

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities.

1.3 Definition of “Client” and “Applicant for Business”

The direct client of Temple Holdings N.V. and applicant for business shall be the player who enters into an agreement with the Company - or with a group company which who a service agreement is in place - by virtue of registration, agreeing to the Terms & Conditions, and funding the player account in order to utilize the Temple Holdings N.V. platform to play games remotely.

For the avoidance of doubt, a player who has registered and agreed to the Terms & Conditions but has not yet funded his player account is not considered to be an applicant for business.

In this scenario, an intermediary of Temple Holdings N.V., who shall enter into a business relationship with Temple Holdings N.V. for the purpose of attracting players to Temple Holdings N.V., shall also satisfy the definition of applicant for business.

1.4 Audience

This AML Policy applies to all employees, officers, directors, contractors, consultants, and any other individuals or entities acting on behalf of the Company, regardless of location or job function.

It is particularly relevant for individuals engaged in the following activities:

- Customer onboarding and due diligence
- Financial transactions and payment processing
- Compliance and risk management
- Legal and regulatory affairs Internal audit and controls
- Sales and account management

All personnel must understand their responsibilities under this policy and complete any required AML training provided by the Company. Failure to comply with the obligations outlined in this policy may result in disciplinary action, up to and including termination of employment or contract.

Third-party partners, agents, and service providers who represent or act on behalf of Temple Holdings N.V. may also be required to comply with this policy, as determined by the nature of their relationship with the company.

Initial


DS


1.5 Law, Regulations and Rules

The Code of Criminal Law (Penal Code) of Curaçao lays down the procedures for the prosecution of a money laundering offence, as well as the measures for the confiscation of property upon a conviction of money laundering, measures for the freezing of assets when a person is charged with an offence of money laundering and measures for the issuance of an investigation and/or attachment order when a person is suspected of having committed an offence of money laundering.

The policies and procedures in this Policy aim to comply with both the rules and guidance contained in the NOPML, the NORUT and the NOIS which regulations themselves are referring to the Penal Code. In addition to these regulations the Curaçao Gaming Board has introduced a comprehensive framework with provisions and guidelines to prevent and combat money laundering and terrorist financing. Curaçao - as a member of the FATF - has based these guidelines on, among others, the FATF recommendations.

1.6 Document Structure

Each section below is divided into the following parts:

- a) The applicable provisions in the NOPML, the NORUT and the NOIS or and CGA regulations;
- b) Guidance on the implementation (where applicable);
- c) Temple Holdings N.V.'s policy in relation to the provisions; and
- d) Procedures and Documentation – the processes by which the policy referred to will be implemented, including reference to other documents as appropriate.

1.7 Consequences of non-compliance

Violations of this AML Policy can expose the Company, its employees, and its partners to significant legal, regulatory, and reputational risks. Understanding and complying with this policy is essential to protect the integrity of our operations and to fulfill our legal and ethical obligations.

Disciplinary Actions

Any employee who fails to comply with this policy may be subject to disciplinary action, which may include:

- Formal warnings;
- Suspension;
- Termination of employment or contract;
- Loss of professional licenses or certifications.

Contractors or third parties found in violation may face termination of agreements and disqualification from future business with Temple Holdings N.V.

Initial


DS


Legal Implications

Non-compliance with AML regulations can result in severe legal consequences, including:

- Civil or criminal prosecution;
- Substantial fines and financial penalties;
- Imprisonment of individuals involved;
- Asset seizures or freezing of funds;
- Disqualification from serving as a company officer or director.

Business and Reputational Risks

Violations can also damage the company's reputation, investor confidence, and customer trust.

Potential consequences include:

- Regulatory investigations or sanctions;
- Loss of partner relationships;
- Increased scrutiny from financial authorities;
- Negative media exposure and reputational harm;
- Financial loss due to operational disruptions or terminated business relationships.

2. AML Systems and Controls – General

2.1 Provisions from the Nois and the Norut

Due Diligence should be applied:

- i) When establishing business relations;
- ii) Where there is a suspicion of ML or TF;
- iii) Where there is doubt about the veracity or adequacy of previously obtained identification data.

The Company is obliged to apply the above measures and procedures including the cases when entering into or undertaking non-face-to-face relationships or transactions directly or indirectly.

The Company is also obliged to establish policies and procedures on risk management practices, internal controls, record keeping, and the monitoring and management of compliance with the aforesaid policies, controls and procedures to adequately and appropriately mitigate risk and prevent the carrying out of operations that may be related to money laundering or the funding of terrorism.

The Company must ensure that employees are made aware of applicable AML/CFT legislation as well as the Company's policies and measures in this regard. Employees of the Company must undergo appropriate due diligence procedures prior to their engagement, when transferred or when promoted. Employees are also expected to be provided with training regarding the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism.

Initial
MC

DS

2.2 Policy

Responsibility

The ultimate responsibility for the AML policy of Temple Holdings N.V. lies with the Director(s). Day-to-day responsibility for the development and implementation of policies and procedures contained within this Policy is delegated to the AML/CFT Compliance Officer.

AML policies and procedures

The policies and procedures operated by Temple Holdings N.V. in order to meet applicable AML and CFT regulatory requirements are documented in this Policy. Policies and procedures will be regularly reviewed to ensure that they continue to meet regulatory requirements and the changing risk environment as per Temple Holdings N.V. as far as applicable.

AML Risk

The AML/CFT Compliance Officer will undertake regular assessments of the money laundering risks and Temple Holdings N.V.'s strategy and success in mitigating those risks.

Temple Holdings N.V. will document its risk management policies and risk profile in relation to money laundering, and its application of those policies in this Policy and in subsidiary documentation referenced herein.

Temple Holdings N.V. uses the following guidance as a base for its AML risk model:

- i. a clear statement of the culture and values adopted towards the prevention of financial crime;
- ii. a commitment to ensuring that identity will be satisfactorily verified in all cases and in a risk based manner, before applicants for business are accepted as clients;
- iii. a commitment to ongoing customer due diligence throughout the business relationship;
- iv. a commitment to ensuring that staff are trained and aware of the law, their legal obligations, and how to meet those obligations
- v. a clear allocation of roles, responsibilities and organizational structure, and recognition of the importance of staff promptly reporting their suspicions internally.

Initial


DS


2.3 Procedures and documentation

Responsibility

The delegated day-to-day responsibility for the AML policy and operation of effective procedures of the Company is documented in the AML/CFT Compliance Officer's Job Description in Annex I below.

Responsibility for the review and update of the AML Policy, and applicable sections, rests with the AML/CFT Compliance Officer and can be delegated to local AML/CFT Compliance Officer if any. Each version of the AML Policy will be reviewed and approved by the Board of Directors prior to being issued and will carry a review and approval date.

AML policies and procedures

The AML Policy is subject to Temple Holdings N.V.'s local and group policies and procedures regarding compliance monitoring, record keeping and reporting.

The AML Policy is reviewed as necessary (but at least annually), updated in order to reflect changes in legislation, national and international findings, the structure of Temple Holdings N.V.'s customers, and the services offered.

The procedures contained in this Policy reflect the Temple Holdings N.V. AML Policy in general and are more specific with respect to the jurisdiction Curaçao and must be adhered to by all staff of the companies belonging to Temple Holdings N.V.

AML risk factors

An AML business risk assessment overview will be maintained in order to allocate and track the components of the separate risk classifications. Temple Holdings N.V. categorizes overall AML risk into:

- Customer risk;
- Geographical risk;
- Product, service and transaction risk; and
- Distribution channels risk

As part of the periodic review of this AML Policy, the AML/CFT Compliance Officer will periodically assess the AML risk for each category in order to develop appropriate mitigating controls.

See Annex II – Risk Assessment below:

Document	Title	Frequency	Audience	Resp.
AML Policy, Annex I	AML/CFT Compliance Officer Job Description	Periodic	Comp. Off., Directors	Compliance Officer
AML Policy, Annex II	Risk Mitigation Matrix and Risk Factors	Periodic	Comp. Off., Directors	Compliance Officer

Initial
MC

DS

3 Risk Assessment, Management and Risk-Based Approach

3.1 Provisions of the NOIS

The Company is required to have policies and procedures in place to mitigate specific risks involved with business transactions or non-face-to-face transactions.

Based on the FATF recommendations and CGA guidelines service providers are allowed to apply a Risk-based Approach ("RBA"). By adopting an RBA, it is possible for service providers to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risk identified. This entails that although all clients should be subject to minimum due diligence standards clients identified by the service provider as high risk must be subject to enhanced customer due diligence while low risk clients may be subject to the simplified minimum prescribed customer due diligence.

3.2 Guidance on Implementation

Risk Assessment

For the implementation of risk-assessment procedures, the AML Regulations recognizes the FATF Standards and that the Company should prepare a risk-assessment, as well as policies, controls, and procedures curated to manage and mitigate ML/FT risks.

The purpose of the risk-assessment procedures is to enable the Company to be in a position to identify and assess the ML/TF risks that the Company is or may become exposed to and thereby determine:

- a) Whether the application of enhanced due diligence is necessary;
- b) The point in time when the application of customer due diligence in accordance with the NOIS to existing customers is to be carried out; and
- c) Whether a customer presents a low risk of ML/FT for the purposes of delaying the performance of verification proceedings to after the commencement of a business relationship, as has been discussed above.

Monitoring Controls

It is essential that the controls to manage and mitigate the identified risks are constantly monitored. This should be done so that in the event of a change in circumstances, which might mitigate or exacerbate a particular risk, the respective control is modified accordingly.

For instance, it is important that the Company has a system in place to identify changes in customer characteristics, as this would obviously have a bearing on the risk profile of the customer. Similarly, the threat posed by a particular product or service may cease to exist, which would lead to a re-consideration of the risk scoring of the business relationship. In view of this, the Company must be in a position to identify such changes.

The Company should also carry out periodic internal audits or assessments to review the adequacy of the risk assessment, the internal controls and the compliance arrangements. Such

Initial
ME

DS

audits or assessments should also review the effectiveness of liaison between the different departments of the organization, and the effectiveness of the balance between technology-based and people-based systems.

3.3 Policy

Risk-based approach

Temple Holdings N.V. operates a risk-based approach to developing and operating its systems and controls designed to prevent financial crime.

AML risk is analyzed, as applicable, into the following risk categories:

- Customer risk;
- Geographical risk;
- Product, service and transaction risk; and
- Distribution channels risk.

The Risk Assessment and Mitigation Matrix in Annex II to this Policy identifies and explains the risks inherent to the particular services provided by Temple Holdings N.V., as well as the actions taken by the Company to mitigate these risks.

The Risk Factor table also in Annex II to this Policy identifies risk factors relevant to Temple Holdings N.V.'s business that indicate a risk of money laundering or terrorist financing.

Risk assessment for the customers is initiated upon reaching the sum of Naf 4,000 (Eur 2,000) with accumulative withdrawal threshold and continuously monitored and re-assessed within the high-risk category. The procedure for arriving at a risk category is set out in Annex II below.

AML risk assessment

The AML/CFT Compliance Officer will perform regular assessments of the AML risks and Temple Holdings N.V.'s local strategy and success in mitigating those risks.

Where a new service, customer group or new geography is addressed by Temple Holdings N.V., the financial crime risk assessment will be updated during development/launch (to ensure that AML processes can support the new activities). In line with article 5h of the NOIS the company will assure that affiliated entities will meet the Curaçao Anti Money Laundering and Terrorist Financing regulations. Such as far as these affiliated entities are affecting the business of the Company in Curaçao. The results of the AML risk assessment will be used to support the development of appropriate systems and controls (policies and procedures) designed to minimize the risk of Temple Holdings N.V., being used for the purposes of financial crime. All developments will be reported to the Board of Directors.

Initial
MC

DS

Risk mitigation

In order to mitigate the risk of money laundering, Temple Holdings N.V. will ensure that appropriate risk-based systems and controls are in place and operated for, amongst others, the Company as prescribed in Annex II below. Existing systems and controls will be reviewed and where necessary amended to reflect changes in assessed risk and identified vulnerabilities. Additional systems and controls will be implemented by the AML/CFT Compliance Officer where required.

Monitoring controls

The AML Policy is subject to Temple Holdings N.V. policies and procedures regarding compliance monitoring. The AML/CFT Compliance Officer will ensure that the internal controls operated by Temple Holdings N.V. are reviewed when there are changes to regulations or Temple Holdings N.V.'s arrangements / products / markets.

When there is a change in the Temple Holdings N.V. AML policies or AML rules in the CGA's AML Regulations this Policy, and associated materials, will be updated and details of the changes included in the AML/CFT Compliance Officer's Annual Report.

3.4 Procedures & Documentation

Risk-based approach

The application of the RBA in the prevention of money laundering is reflected in the Temple Holdings N.V.'s approach to the operation and development of the systems and controls designed to minimize the risk of the Temple Holdings N.V. being used for the purposes of financial crime. Risk is central to the development of the business, new products, development of product functionality or the operation in new markets. The risk-based approach is referenced in all Temple Holdings N.V.'s AML documentation.

AML risk assessment

AML risk assessments are undertaken on an ongoing basis, and in particular, applied when the business environment changes through, for example:

- Entry into new markets; and
- Development of new products or product features / functionality.

Risk mitigation activities, i.e. the development of appropriate internal controls, flow from the findings of the risk assessments.

Risk assessments and the development of mitigating actions are documented in Annex II below and are accordingly reported to the Board of Directors.

Initial


DS


Risk mitigation

Temple Holdings N.V. seeks to minimize the opportunities for carrying out financial crime, i.e. money laundering or funding of terrorism, and to then address and mitigate any risks that remain as further set out in Annexes II and III below.

Internal controls focus on:

- Due diligence of clients, including levels of enhanced due diligence based on risk assessments of each customer;
- Assessing risks and setting out measures to mitigate the said risks;
- Monitoring key risk factors for reassessing a specific customer's risk;
- Financial crime systems and controls will continue to be developed over time in order to adequately address the changing risk environment.

Monitoring controls

This Policy is reviewed and, if necessary, updated continuously in order to reflect changes in the AML policies and procedures which affect the operations of Temple Holdings N.V. Consequently, the AML/CFT Compliance Officer's regularly reviews the following areas.

- a) Developments in legislation, including the NOIS; and the NORUT.
- b) Financial crime risk assessments – whose performed as part of the development of new products, services, functionality or addressing new customers / markets.
- c) The operation of periodic internal controls, including monitoring, investigation and reporting of unusual activity.
- d) New typologies for fraud or financial crime, including feedback from regulators or law enforcement.
- e) Feedback received following the provision of training or Compliance reports to the Board by the AML/CFT Compliance Officer.

Document	Title	Frequency	Audience	Responsibility
Report	AML/CFT Compliance Officer Internal Audit Report	Annual	Board	AML/CFT Compliance Officer

Initial


DS


4. Customer Due Diligence

4.1 Guidance from CGA Regulations

Casinos have the obligation to undertake Customer Due Diligence measures when:

- a) When players engage in financial transactions equal to or above Naf. 4,000;
- b) carrying out occasional transactions above the monetary equivalent of NAF. 4,000;
- c) there is a suspicion of money laundering or terrorist financing; or
- d) the casino has doubts about the veracity or adequacy of previously obtained customer identification data.

4.2 Guidance on implementation

The CDD measures to be taken are as follows:

- Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, its source of funds.

Notwithstanding this, the NOIS allows subject persons to delay the verification of the identity of the applicant for business and, where applicable, the identity of the beneficial owner until after the establishment of a business relationship where this is necessary for the continued normal conduct of business provided that the risk of money laundering or the funding of terrorism is low and, provided further, that the verification procedures be completed as soon as is reasonably practicable after the initial contact. Regulations add that in the event that customer due diligence measures are applied after the establishment of a business relationship, subject persons should record the reasons for deferring the application of customer due diligence measures. A determination on whether the risk of money laundering or funding of terrorism is low should be based on mandatory risk procedures.

Initial


DS


4.3 Policy

Customers of the Company are subject to risk-based initial and ongoing due diligence procedures according to the risk categories outlined in Annex II below and the Customer due diligence procedures set out in Annex III below.

Initial due diligence seeks to obtain the identity of the customer and verify the identity prior to the establishment of the business relationship. Information on the purpose and intended nature of the business relationship, is also obtained, such that the Company is able to establish the business and risk profile of the customer and to accept or reject a client based on the Client Acceptance Policy set out in Annex IV below. Ongoing procedures ensure that the initial due diligence information remains up to date.

4.4 Procedures and Documentation

The detailed procedures for the performance of risk-based customer due diligence are detailed in Annex III below relating to Customer Due Diligence.

Document	Title	Frequency	Audience	Responsibility
AML Policy, Annex II	Risk Mitigation Matrix and Risk Factors	As required	Relevant staff	AML/CFT Compliance Officer
AML Policy, Annex III	Customer Due Diligence	As required	Relevant staff	AML/CFT Compliance Officer
AML Policy, Annex IV	Client Acceptance Policy	As required	Relevant staff	AML/CFT Compliance Officer
Terms and Conditions	Services Agreement	As required	Relevant staff	AML/CFT Compliance Officer

5. Ongoing monitoring

5.1 Provisions from the Regulations

The casino must conduct ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the casino's knowledge of the customer, the customer's business and risk profile.

5.1.1 *Ongoing monitoring of identity*

"In conducting ongoing due diligence on the business relationship, the casino should hold accurate and up to date identification data of its customers. Since identity may change due to circumstances, the casino should be able to demonstrate that if identification information changes, it will be detected and re-evidenced."

5.1.2 *Ongoing monitoring of transactions*

"Transaction monitoring is executed to prevent involvement of the casino with ML/TF and to safeguard the reputation of the casino. While performing ongoing scrutiny of transactions a casino notices that a customer's transactions are not consistent with what it knows or expects from the customer, the casino has to question this unusual activity and, where necessary, establish the source of the funds used for these transactions."

5.2 Guidance on Implementation

The NOIS states that once the business profile of a customer has been established, ongoing monitoring enables subject persons to identify any unusual transactions which may involve ML/FT. This gives greater assurance that the activities of the subject person are not being misused for the purposes of ML/FT. The regulations provide further that ongoing monitoring of a business relationship includes:

- a) the scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, his business and risk profile, including where necessary, the source of funds; and
- b) ensuring that the documents, data or information held by the subject person are kept up to date.

Paragraph (a) above requires subject persons to collect the necessary information to ensure that the customer's business corresponds to the information disclosed by the customer at the beginning of the business relationship and that the business patterns of the customer are consistent with the risk profile established by the subject person. Where it is revealed that the customer's business and risk profiles have significantly diverged from the established patterns or for no apparent economic or lawful purpose, action should be taken in accordance with the internal procedures of the subject person. This should be conducive to reviewing the risk profile of the customer and considering whether reporting is necessary.

Thus, as a result of the introduction of systems and procedures to ensure ongoing monitoring, activities which do not conform to the established business and risk profiles of the customer

Initial
MC

DS

are immediately brought to the attention of the AML/CFT Compliance Officer. The AML/CFT Compliance Officer would then be in a position to assess whether there is a suspicion of ML/FT and whether that suspicion warrants a report to the FIU in terms of article 2d of the NOIS and article 11 paragraph 1 of the NORUT.

In order to fulfil the obligation, set out in paragraph (b) above, subject persons are required to have a system in place to keep up-to-date documents, data or information held in the fulfilment of their CDD obligations, including information and documents obtained by the subject person. in order to fulfil the obligation set out under article 6 of the NOIS. This should include the updating of expired documentation. This ensures that in the event of an analysis or investigation of ML/FT the subject person is in a position to provide accurate and updated information to the FIU or the Police.

5.3 Policy

Ongoing monitoring processes will focus on ensuring that due diligence information provided is up to date and that no documentation is expired. On-going monitoring will also ensure that there have been no material changes to the Client that affects the risk profile of the Client.

On-Going Monitoring Measures

On-Going Monitoring will be conducted on a continual basis for all Customers. On-Going Monitoring will include:

- Ongoing Screening: Daily/Weekly screening against all relevant sanctions, PEPs, and adverse media lists.
- Periodic Review: Periodic Reviews will be commensurate to the ML/TF risk associated with the Customer.
- Event Driven Reviews (“EDR”): An EDR will be initiated on the identification of a high-risk factor or red flag during the ongoing monitoring process (including Transaction Monitoring).

Due Diligence information

Due diligence information will be reviewed as follows to ensure that it remains up to date.

Low Risk Customers:	Once every 2 years
Medium Risk Customers:	Annually
High Risk Customers:	Quarterly

5.4 Procedures and Documentation

The Company notes that it offers a single service to its customers whereby the applicant for business is affecting payments for remote gambling services. Therefore, in all cases, the Company understands the nature of the relationship with the customer and all payments received are sourced from this business.

Initial
ME

DS

Training will be provided to relevant staff to ensure that they are aware of the requirement to stay alert to the possibility of unusual activity and what unusual activity might comprise. Training is addressed in Section 9 below.

Customer initial due diligence information set out in Annex III will be periodically reviewed to ensure that it remains up to date as per the above. This review is recorded by way of assessing whether any due diligence information has expired.

The review will also assess whether any changes have been made to the company structure and/or the people involved. In such an instance, due diligence will be updated accordingly.

6 Reporting

6.1 Provisions from the CGA's AML regulation

Casinos are not only required to adhere to the stipulations of the National Ordinance for Identification of Services, but are also required to detect and report either intended or completed unusual transactions. It is important that every casino has adequate procedures in place that cover the following:

- The recognition of unusual transactions;
- The documentation of unusual transactions; and
- The reporting of unusual transactions.

As regards external reporting, the NORUT provides:

Where a subject person knows, suspects or has reasonable grounds to suspect that a transaction may be related to money laundering or the funding of terrorism, or that a person may have been, is or may be connected with money laundering or the funding of terrorism, or that money laundering or the funding of terrorism has been, is being or may be committed or attempted, that subject person shall, as soon as possible, disclose that information, supported by the relevant identification and other documentation, to the Financial Intelligence Analysis Unit.

6.2 Guidance on Implementation

Internal Reporting

If the AML/CFT Compliance Officer concludes, for justifiable reasons, that an internal report does not give rise to a suspicion, the AML/CFT Compliance Officer need not to inform the FIU. In this case, the AML/CFT Compliance Officer shall keep a written record of the internal reports received, the assessment carried out, the outcome and the reasons why the report was not submitted to the FIU. Upon request by the FIU or the relevant supervisory authority acting on behalf of the FIU, or in completing the Annual Compliance Report, the AML/CFT Compliance Officer will make such information available.

Initial
MC

DS

Offences Committed Outside Curaçao

According to article 5h paragraph 1 of the NOIS the Service Provider should take care and organize that its foreign subsidiaries and branches, if any, are meeting the requirements of the NOIS. In case and as far as the legislation of the involved jurisdiction does not allow the NOIS measures the Service Provider should inform the Regulatory Authority followed by actions of the Service Provider to avoid the risks of ML/TF.

6.3 Policy

Annual Compliance Report and AML/CFT Compliance Officer Report

Each casino has to register with the FIU and to obtain access to the goAML reporting portal after validation by the FIU. The FIU allows bulk reporting, therefore the casino account manager at the FIU should be contacted in order for the FIU to determine if the operator qualifies for this service.

The AML/CFT Compliance Officer shall also prepare a report to be presented to the Directors to outline issues pertinent to the management of financial crime, of which the Board should be aware. This AML/CFT Compliance Officer Report is for internal purposes and does not need to be submitted to the FIU.

Internal Reporting

Temple Holdings N.V.'s reporting policy applies to the 'relevant staff' of Temple Holdings N.V., Providers and Distributors. Relevant staff are those that handle or who are managerially responsible for handling, or are otherwise 'close', to customer transactions or accounts.

Temple Holdings N.V. will generate two types of unusual activity reports:

- **Internal UTRs** - Internal unusual activity reports may be generated by all relevant staff. Internal UTRs are used to report unusual activity to the AML/CFT Compliance Officer, and
- **External UTRs** - External unusual activity reports are produced by the AML/CFT Compliance Officer in the event of unusual activity having been identified and confirmed through investigation. External UTRs are submitted to the FIU. *Each casino has to register with the FIU and to get access to the goAML reporting portal after validation by the FIU.*

Records relating to both Internal and External UTRs are kept in accordance with Temple Holdings N.V.'s record-keeping policy. External UTRs are kept for a minimum period of 5 years.

All relevant staff will receive both initial and ongoing training on anti-money laundering, detection of unusual activity and the internal reporting process.

Initial
MC

DS

Internal Reporting - Temple Holdings N.V. Staff

Where a Temple Holdings N.V. staff member knows or suspects, or has reasonable grounds for knowing or suspecting, that any customer is engaged in money laundering, they must report these suspicions to the AML/CFT Compliance Officer using the Temple Holdings N.V. Unusual Transaction Reporting Form.

Any Temple Holdings N.V. staff member that does not adhere to the internal reporting requirements will be subject to disciplinary process.

Internal Reporting – Providers and Distributors

Where any relevant staff member in a Provider or Distributor, knows or suspects, or has reasonable grounds for knowing or suspecting, that any customer is engaged in money laundering, they should report their suspicion directly to the Temple Holdings N.V. AML/CFT Compliance Officer.

External Reporting (AML/CFT Compliance Officer)

Where an unusual activity report has been made to the AML/CFT Compliance Officer he will conduct investigations and access information on the customer, or the transaction, as necessary.

Where appropriate, an UTR will be made to the FIU by the AML/CFT Compliance Officer which will include the mandatory information. In the file format and following the instructions available from the FIU. The UTR can be filed through the FIU's goAML portal or by means of a manual report form ([http://: www.mot.cw](http://www.mot.cw)).

6.4 Procedures and Documentation**AML/CFT Compliance Officer Role**

The responsibilities associated with the AML/CFT Compliance Officer role are documented in the AML/CFT Compliance Officer Job description.

To ensure that Temple Holdings N.V. maintains an AML approach that meets regulatory requirements, the AML/CFT Compliance Officer will regularly review developments in legislation and their impact on the policies and procedures contained in this Policy, including:

1. Curaçao legislation (CGA regulations);
2. National and International Findings; and
3. Local legislation in the countries of relevant Providers and Distributors.

If changes in the Curaçao anti-money laundering legislation are found to contribute to an increased risk of money laundering, through the periodic performance of a financial crime risk assessment, the policies and procedures in this Policy will be updated by the AML/CFT Compliance Officer. The AML/CFT Compliance Officer communicates changes in policies and procedures to all relevant parties.

Initial
MC

DS

In order to ensure that Temple Holdings N.V. AML approach addresses current AML risk, the AML/CFT Compliance Officer undertakes regular financial crime risk assessments and considers the Temple Holdings N.V. strategy and success in mitigating those risks, using the risk categories detailed in Annex II. The performance of risk assessments is detailed in Section 3 above. The results of these periodic assessments will be regularly reported to the Board of the Company.

Internal Reporting

Relevant staff will receive initial and periodic training to ensure that their reporting obligations, and the method of making an Internal UTR, are understood as well as to assist them to recognize unusual activity. Typologies are maintained and will be used as part of the training provided.

Internal UTRs should be sent to the AML/CFT Compliance Officer using the 'Temple Holdings N.V. Unusual Transaction Reporting Form'. The AML/CFT Compliance Officer acknowledges the receipt of all Internal UTRs and will provide a reminder regarding tipping off requirements to the person making the report.

The AML/CFT Compliance Officer will investigate all reported unusual transactions in light of all available information and document the findings, regardless of whether or not an external UTR is made. All documented information will be retained with the Temple Holdings N.V. Unusual Transaction Reporting Form and retained in order to provide documentary evidence of the investigation process. Any further attempted activity on an account where an internal UTR has been made must be reported to the AML/CFT Compliance Officer to ensure that appropriate action is taken in order to avoid tipping off.

External Reporting

An external UTR is triggered when, after investigation by the AML/CFT Compliance Officer, a transaction, transaction pattern or account activity is deemed unusual and suggests potential criminal activity. External UTRs will be sent to the Curaçao FIU.

7 Record-Keeping Procedures

7.1 Provisions from the NOIS and the NORUT

Regulation of the NOIS provides that the following records are to be kept for a period of at least five years by the subject person:

- a) in relation to any business relationship that is formed or an occasional transaction that is carried out, a record indicating the nature of the evidence of the customer due diligence documents required and obtained under procedures maintained in accordance with these regulations, comprising a copy of or the reference to the evidence required for the identity and providing sufficient information to enable the details as to a person's identity contained in the relevant evidence to be re-obtained;
- b) a record containing details relating to the business relationship and to all transactions

Initial
ME

DS

carried out by that person in the course of an established business relationship or occasional transaction which shall include the original documents or other copies which are admissible in court proceedings;

- c) a record of the findings of the examination of the background and purpose of the relationships and transactions therein.

7.2 Guidance on Implementation

The regulations provide that generally, records may be kept in any of the following forms:

- in physical files;
- in scanned form;
- in computerized or electronic form.

Subject persons should use a standardized approach to record keeping and must ensure that the approach used enables the quick retrieval of records.

7.3 Policy

The AML/CFT Compliance Officer is responsible for specifying which AML records must be retained and for ensuring that all such records are retained in accordance with Temple Holdings N.V.'s record-keeping policy. Records may be held in paper-based and/or electronic form and stored by the Company. The Company will ensure that all AML records are retrievable without undue delay. Records must be kept for a minimum of **5 years** (may be extended to 10 years if required by the FIU). The table below provides guidance on the types of records that must be retained and their respective retention periods.

7.4 Procedures & Documentation

The below timeframes do not relate to accounting records which, in terms of Book 2 of the civil code of Curaçao are to be retained by the company for a period of 10 years:

Record	Content	Location	Responsibility
Outsourcing	SLAs or contracts, details of contact persons, training records, any relevant information about local anti-money laundering legislation.	Temple Holdings N.V.	Key Official

Record of Customer Due Diligence	Identity of clients; Identity of directors, beneficial owners, business proposition, expected transaction levels	Temple Holdings N.V.	AML/CFT Compliance Officer
Internal & external unusual transaction reports	All actions, information not acted upon, UTRs made	Temple Holdings N.V.	AML/CFT Compliance Officer
AML Training	Dates, nature of training, names of attendees, results. To be stored in the personnel files.	Temple Holdings N.V.	AML/CFT Compliance Officer
AML Policy	Previous versions of the AML Policy	Temple Holdings N.V.	AML/CFT Compliance Officer

8. Awareness and Training

8.1 Provisions from the NOIS

Casinos must take appropriate measures from time to time for the purpose of making employees aware of said subject person's AML/CFT policies and procedures as well as relevant legislation.

The NOIS also provide that a subject person must provide "...employees from time to time with training in the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism."

8.2 Guidance on Implementation

Regulations state that all employees should be made aware of the subject person's:

- customer due diligence measures;
- record-keeping procedures;
- internal reporting procedures;
- policies and procedures on internal controls;
- policies and procedures on risk assessment and risk management; and
- policies and procedures on compliance management and communication.

Employees should also be made aware of the following:

- CGA regulations (including the provisions of the NORUT and the NOIS);
- the provisions in the Criminal Code on ML & TF;

Initial
MC

DS

- the provisions of the P&G;
- the offences and penalties in relation to any breach of the NOIS or the NORUT

All the above-mentioned information should be made readily available to all employees to enable them to refer to such information as and when appropriate throughout the conduct of their duties. The P&G highlights that training should be tailored in accordance with the specific responsibilities and functions of the respective employees and the business carried out by the subject person. For instance, front-office employees should be provided with a different kind of training to that provided to employees carrying out back-office functions and the training provided by a credit institution would naturally differ from the training provided by a company carrying out the business of insurance or a real-estate agent.

Additionally, training should be of a more practical nature rather than simply theoretical. This means that the training provided should make references to real-life situations such as, for instance, the steps to be followed when accepting customers, the handling of high-risk customers and the behavior to be adopted when faced with a request for a transaction which is suspicious. Typology reports prepared by the FATF or Moneyval play an important role in preparing training material.

Casinos need to determine the method in which training is to be delivered, as the most appropriate method may vary from one organization to the other. The method generally depends on the size of the organization. Online learning systems can often provide an adequate solution for general training to all employees who deal with clients, while focused classroom training for higher- risk areas can be more effective.

It is vital to maintain comprehensive records of training sessions which, should include:

- a) the date on which the training was delivered;
- b) the nature of the training;
- c) the names of employees receiving the training;
- d) the results of any assessment undertaken by employees; and
- e) a copy of any handouts or slides.

8.3 Policy

The Temple Holdings N.V. AML/CFT Compliance Officer is responsible for ensuring that all relevant staff received training that effectively communicates Temple Holdings N.V.'s AML and CFT responsibilities and the policies and procedures that are operated to ensure that those responsibilities are met.

Relevant persons

Relevant staff include the staff of the Company who handle or are managerially responsible for the handling of customer on-boarding and service provision.

Training

Training will be designed to ensure that all relevant staff are made aware of the risk of the Company being used for the purposes of financial crime, the consequences for the firm (as well as staff personally), the requirement to operate systems and controls to mitigate such risk and

Initial
MC

DS

the requirement to report unusual activity to the AML/CFT Compliance Officer.

The frequency of the provision of AML training will be determined using a risk-based approach, with those who may be at greatest risk from handling unusual transactions, or who need to be kept up-to-date with changing vulnerabilities and trends, receiving training at more frequent intervals; relevant staff who are close to transaction processing activity are prioritized for training which may be more detailed in content than the training provided for other staff.

Where applicable, provision for AML training will be made in the contractual arrangements, or Service Level Agreements, between Temple Holdings N.V. and its partners.

AML/CFT Compliance Officer training

The AML/CFT Compliance Officer will keep up to date with legislative changes in Curaçao and on international level and industry standards in order to guide and develop appropriate training for relevant staff.

8.4 Procedures & Documentation

Relevant persons

The AML/CFT Compliance Officer will maintain a record of Temple Holdings N.V. staff, and their positions within the company, for use when deciding which individuals are 'relevant staff' and, further, which will require more frequent and more detailed training due to the nature of their specific role.

Training

All relevant staff will be provided with an awareness of Temple Holdings N.V.'s AML policies and processes through the provision of AML training. Relevant staff will be provided with initial AML training within one month of their taking up relevant activities on behalf of Temple Holdings N.V. Priority is given to those staff responsible for handling or managing the handling of transactions or customer accounts.

All relevant staff must acknowledge that they have read and understood the training that is provided, to be recorded in the AML Staff Training Log.

The frequency of training provided to each staff member is determined by the AML/CFT Compliance Officer with reference to the staff member's role. Refresher training is repeated at appropriate intervals. Relevant staff are tested on the AML training received.

Training materials are updated by the AML/CFT Compliance Officer when required to reflect new developments. Training materials and records are retained in accordance with the Company record-keeping policy.

AML training will be delivered to relevant staff and will include the following elements:

1. Legal and regulatory obligations under Curaçao law;
2. Practical means of identifying unusual transactions; and
3. Internal processes and advice on how to act when presented with unusual activity.

Initial
MC

DS

AML/CFT Compliance Officer training

The AML/CFT Compliance Officer will receive external training as appropriate and is required to evidence, to the Board, their further professional development (using the AML/CFT Compliance Officer Annual Report).

Document	Title	Frequency	Audience	Responsibility
Presentation	AML Awareness & Training Presentation	Annually	All staff	AML/CFT Compliance Officer
Log	AML Staff Training Log	Periodic	AML/CFT Compliance Officer	AML/CFT Compliance Officer

8.5 Anti-Bribery & Corruption Policy

The Company has embedded this Anti-Bribery & Corruption (ABC) Policy within the main AML Policy under this section. It outlines the commitment of Temple Holdings N.V. to conducting its business activities in an ethical and lawful manner. The Company is dedicated to prevent bribery and corruption in all its operations and is committed to fostering a culture of integrity, transparency, and compliance.

The Company prohibits all forms of bribery and corruption, whether direct or indirect, and expects its employees, associates, contractors, and business partners to adhere to the highest standards of integrity and ethical behavior. This part of the policy applies to all employees, contractors, agents, suppliers, partners, and any individual or entity associated with the Company's operations, regardless of their role or position.

Definitions

Bribery: The offering, giving, receiving, or soliciting of any item of value (including but not limited to money, gifts, favors, entertainment, or services) to influence the actions of an individual in a position of trust or authority.

Corruption: The abuse of power or authority for personal gain, often involving bribery, embezzlement, fraud, or other unethical practices.

Associated Persons: Any individual or entity that has a business relationship with the Company, including employees, contractors, agents, suppliers, partners, and third-party intermediaries.

Prohibited Conduct

a. **Bribery and Corruption:** No employee or associated person shall engage in any form of bribery, corruption, or unethical behavior. This includes offering, promising, giving, receiving, or soliciting bribes or other improper benefits.

b. **Gifts and Hospitality:** Employees and associated persons must not offer or accept gifts, hospitality, or entertainment that could be seen as an attempt to influence business decisions or compromise the recipient's judgment.

Initial
ME

DS

c. Facilitation Payments: Facilitation payments (small unofficial payments to expedite routine processes) are strictly prohibited. Employees and associated persons must not make or accept such payments.

The Company is committed to conduct thorough due diligence on all third parties before entering into business relationships with them. This includes assessing their integrity, reputation, and compliance with anti-bribery laws. Violations of this policy will not be tolerated and may result in disciplinary action, up to and including termination of employment or business relationships. In severe cases, legal action may be pursued. This policy will be reviewed periodically to ensure its effectiveness and relevance. Any necessary updates will be made to reflect changes in laws, regulations, and the Company's operations.

9. The screening process

The screening of potential customers against sanctioned persons, against PEPs is carried out by Temple Holdings N.V. via a 3rd party Provider, a holistic and seamless Customer Due Diligence software.

Sanctions and PEP screening result: on each possible match by selecting the entity result, positive hits.

To screen customers, the Company selects the screening icon and inserts the customer details requested. Once this is done, the Company will be presented with the possible results together with searches conducted via third party screening as well as targeted google searches.

In addition to the identification and verification procedures, external search checks will be performed on the customer through the 3rd party provider's platform. Selecting the search engine item link shall direct the Company to another screen providing the actual information found within that link.

The Company is obliged to undertake measures at law aimed at combating terrorism, terrorism financing and the financing of the proliferation of weapons of mass destruction. This includes obligations emanating from the National Interest (Enabling Powers) Act relating to sanctions screening, freezing of assets and reporting.

Initial


DS


10. Sanctions Lists

10.1 Guidance on Implementation

According to CGA regulations service providers must take into account available information including any (updated) lists that for the purposes of fulfilling the obligation imposed on subject persons to combat the funding of terrorism, subject persons should, inter alia, have a system in place which detects whether an applicant for business is subject to any financial sanctions issued by, amongst others:

- EU Sanctions List - <https://www.sanctionsmap.eu/#/main>;
- The listing of the Office of Foreign Assets Control (OFAC) - <https://sanctionssearch.ofac.treas.gov/>; and
- The UN Sanctions List - <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>.

Such system should be sufficiently adequate for subject persons to keep themselves updated with all sanctions that might have an impact on their business operations.

10.2 Policy

Sanctions list screening is the responsibility of the AML/CFT Compliance Officer. The performance of the screening procedures may be delegated or outsourced.

In obtaining, applying, and disseminating government and FATF findings, the AML/CFT Compliance Officer ensures that all customers and business partners (e.g. Distributors) with whom a business relationship is established, are subject to due diligence procedures that ensure screening against relevant notices published by the OFAC, FIU and FATF.

Sanctions screening will form part of the initial due diligence procedures as well as the ongoing monitoring of customers and business partners as detailed in Annexes III and IV below. 'False positives' are investigated, and **any true sanction matches reported to the AML/CFT Compliance Officer immediately.**

Staff are required to report where they have knowledge or a suspicion that financial sanctions measures have been or are being contravened.

10.3 Procedures and Documentation

All customers shall be subject to Sanctions screening once this is actively implemented as part of the initial due diligence procedures, with all customers being rechecked regularly as part of the ongoing monitoring of customers. Staff responsible for performing Sanctions checks will receive specific training. Matches will be investigated by staff in order to identify true matches from those that are 'false positive'. All true sanctions matches must be reported to the AML/CFT Compliance Officer immediately, using the Internal Unusual Transaction Reporting Form and followed up by an email thereafter.

Initial
MC

DS

11. Politically Exposed Persons

11.1 Provisions from the NOIS

Article 5a of the NOIS states: "...where the applicant for business or the beneficial owner is subsequently found to be or becomes a politically exposed person, customer due diligence shall proceed in accordance with article 5b of the NOIS."

Appendix 1 of the P&G defines "politically exposed persons" as individuals who are or have been entrusted with promoting public functions, including heads of states or of governments, senior politicians, senior government, judicial or military officials, senior executives or publicly owned corporations and important political party officials.

11.2 Guidance on Implementation

In relation to PEPs the P&R indicates that service providers must have appropriate risk management in place to determine whether it's (proposed) clients are considered political exposed persons ("PEP's) and must conduct enhanced due diligence for PEPs, their families and associates. The service provider's decision to enter into business relationships with a PEP must be taken at its senior management level. The service provider must make reasonable efforts to ascertain that the PEPs source of wealth and source of funds/income is not from illegal activities and where appropriate review the customer's credit and character and the type of transactions the customer would typically conduct. Service providers must not accept or maintain a business relationship if the service provider knows or must assume that the funds are derived from corruption or misuse of public assets. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, institutions must obtain senior management's approval to continue the business relationship. Where the institution is in a business relationship with a PEP, it must conduct enhanced ongoing monitoring on that relationship.

11.3 Policy

It is Temple Holdings N.V.'s policy not to accept PEPs as customers and the Company will proceed to end the relative business relationship with any individual/s found to be PEPs (notwithstanding declaring otherwise in the onboarding process).

Risk assessments for new customers, products or features will take account of the risk that the product might be used by PEPs for money laundering purposes.

11.4 Procedures and Documentation

A third-party check shall be carried out on each person to assess whether the person in question is a PEP.

Initial
MC

DS
[Signature]

Annex I – AML/CFT Compliance Officer Job Description

AML/CFT Compliance Officer

Responsibility

Temple Holdings N.V. is responsible for appointing an AML/CFT Compliance Officer of appropriate seniority with access to the resources required to effectively perform the role. Resources include time, support staff, the freedom and independence to act on authority, and access to relevant data / information.

In summary, the Board of the Company delegates the following high-level responsibilities to the AML/CFT Compliance Officer:

- Establishing and operating appropriate risk-based internal policies, procedures and controls to prevent money laundering or terrorist financing, consistent with legal and regulatory requirements as set out in Curaçao and international provisions.
- Reviewing, updating and approving AML and CFT policies based on an assessment of risk and its management, ensuring that such assessments are kept up to date.
- Ensuring that priority is given to the implementation of AML and CFT policies and take ultimate responsibility for the development and operation of procedures that implement policy.
- Maintain up-to-date documentation detailing the risk-based AML and CFT arrangements operated by the Company.

AML/CFT Compliance Officer Role

The AML/CFT Compliance Officer may delegate certain functions, in particular those related to the day-to-day monitoring of procedures and systems to detect unusual activity, to suitable individuals in Temple Holdings N.V. (where resources are available).

It is the AML/CFT Compliance Officer's ultimate managerial responsibility to ensure that the provisions of this Policy are enforced. Where the AML/CFT Compliance Officer delegates any activities, he will remain accountable for the operation of the delegated functions.

The AML/CFT Compliance Officer may hold other senior management responsibilities within entities of Temple Holdings N.V., to the extent that they do not interfere with their ability to conduct the AML/CFT Compliance Officer duties.

In the absence of the AML/CFT Compliance Officer for a period of less than 12 weeks, the AML/CFT Compliance Officer duties will be temporarily performed by a suitably experienced and qualified individual from within Temple Holdings N.V. The AML/CFT Compliance Officer will always remain reachable and in close contact with the head office.

Should the position of the AML/CFT Compliance Officer become vacant (i.e. the AML/CFT Compliance Officer be absent for a period of 12 weeks or more in a consecutive 12-month period), the Board will appoint another individual as its AML/CFT Compliance Officer.

Initial


DS


POSITION RESPONSIBILITIES

Establishing and supervising AML and CFT systems and controls

Developing and overseeing the implementation of appropriate **AML and CFT policies and procedures**.
 Determining the level of **resources** required to execute appropriate AML and CFT policies and procedures.
 Maintaining and developing the **risk-based approach** to AML and CFT arrangements - carrying out regular **assessments** of the adequacy of systems and controls.
 Reviewing the output from the **unusual activity monitoring** processes.
 Ensuring that AML and CFT requirements are considered as **part of the development** of new products, or service changes.
 Obtaining Board approval for significant **process changes**.
 Ensure that policies and procedures are accurately documented in the **AML Policy** which should be available to staff and used to guide training.
 Ensure that the Board are kept informed of the **money laundering risks** posed by the business and its activities, and how these are managed and mitigated.
 Reporting to the Board on a regular basis detailing the operation and effectiveness of the systems and controls used to combat financial crime.
 Documenting and ensuring that any actions recommended by the Board are **implemented**. Arranging and assisting with **regulatory visits** and **audit inspections**.

Maintaining relevance of the AML systems

Regularly reviewing developments in applicable **legislation and guidance** (domestic and international where the business is involved).
 Ensuring that **policies and AML are updated** to meet changing regulatory and business requirements.
 Ensuring that the operation of systems and controls are **monitored** and that they implement policy. Ensuring that relevant staff are provided with **training** appropriate for their position (frequency and content) and that all new staff receive training within the specified period. Ensure that **training materials** remain up-to-date and relevant to the business.

Reporting unusual activity

Investigating **internal Unusual Transaction Reports (UTRs)**.
 Deciding, following investigation, whether the internal report gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion and submitting an **external UTR to the Curaçao Financial Intelligence Unit (FIU)** where appropriate.
Documenting the reasons for not submitting an external UTR to FIU and/ where an internal report has been made, considered and deemed not to be suspicious.
 Maintain a **filing system** of all internal UTRs, separating between those reported to FIU and those not. Ensure that relevant **records are retained** for the prescribed periods. Where required be the main **point of contact** for law enforcement officials.

Initial
MC

DS
[Signature]

Annex II – Risk Mitigation Matrix and Risk Factors

Risk Assessment and Mitigation Matrix

Risk Number	Risk Identification	Current mitigating controls	Residual risk as a result of mitigations	Comments
R001	High, or no transaction or transfer limits may be linked to money laundering;	Application of transaction limits on individual transactions (See Annex VI). In addition, payments originate only from bank accounts (no cash)	Medium	None
R002	Frequent cross-border transactions can give rise to difficulties with information sharing;	All cross-border transactions originate only from bank accounts (no cash). High Risk Jurisdictions are also subject to enhanced due diligence (see Annex III below)	Low	None
R003	Some betting, gaming activity pose a higher risk of money laundering. This is because of the higher amounts of funds that are transacted and because of the opportunities presented within that environment;	All cross-border transactions originate only from bank accounts (no cash). High Risk Jurisdictions are also subject to enhanced due diligence (see Annex III below)	Medium	None

Initial
ME

DS
[Signature]

R004	Transfers by unverified parties presents a higher risk of money laundering, whether it is the customer who is unverified or a third party;	Details on the customer (including bank account, name and surname) are received from the bank from which bank transfers originate	Low	None
R005	Transfers using cash offers little or no audit trail of the source of the funds and hence presents a higher risk of money laundering;	All transactions to and/or from Clients are by bank account (or authorized payment institutions)	Low	Cash is not accepted
R006	The non face-to-face nature may give rise to increased risk, such as impersonation fraud;	Application of Customer Due Diligence verification to non face-to-face customers (see Annex III)	Low	None
R007	Increased product functionality may in some instances give rise to higher risk of money laundering (product functionality includes person-to-business, person-to-person, and business-to-business transfers);	Clients are all individuals and therefore there is limited product functionality	Low	None

Initial
MC

DS
[Signature]

R008	Products that feature multiple cards linked to the same account increase the utility provided to the user, but may also increase the risk of money laundering, particularly where the customer is able to pass on linked 'partner' cards to anonymous third parties;	All transactions to and/or from Clients are by bank account (or authorized financial institutions)	Low	Transactions by same customer with multiple cards are analyzed and copies of cards are requested.
R009	Segmentation of the business value chain, including use of multiple agents and outsourcing, in particular to overseas locations, may give rise to a higher risk;	All transactions to and/or from Clients are by bank account (or authorized financial institutions)	Low	No agents and limited outsourcing.
R010	Transfer of funds from or to countries with high levels of organized crime or drug production/distribution.	IP blocking is applied	Medium	None
R011	Making funds available to persons subject to financial sanctions.	Sanction checks shall be carried out on Clients as part of onboarding procedures and ongoing monitoring	Low	None

Initial
MC

DS
[Signature]

R012	Customers who are in a public position and/or location which carries a risk of exposure to the possibility of corruption.	PEPs shall be identified via third party database. Application of Enhanced Due Diligence to PEPs including requirement to provide source of wealth and funds.	Low	None
R013	Transmission of money from or to individuals, organizations or locations that may be linked to terrorist activity.	Application of transaction limits on individual transactions (See Annex VI). Payments originate only from bank accounts or authorized financial institutions (no cash). Also, CDD measures and noting of commercial activity.	Low	

Risk Factors Table

The below represented risk factors relevant to Temple Holdings N.V.'s current service offerings that could indicate Money Laundering or Funding of Terrorism as per the risks highlighted in the table above.

Risk Factor	Risk Factor	Risk score	Mitigating Reasons
Customer	PEP/Sanctioned	10	None
Customer	Customers based in or conducting business in, or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime or drug production/distribution	10	None
Geographical Area	Merchant's customers are based in or conducting business in, or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime or drug production/distribution	10	None

Initial
ME

DS
[Signature]

Process for Determining Customer Risk (to be implemented)

The activities of each customer, the product, the distribution channels and the geographic area are assessed in relation to the risk factors above and the said assessment is recorded. A proposed risk assessment of Low, Medium or High is recorded whereby a low risk assessment is awarded to a customer with a 0-3 risk score, a medium risk assessment to a customer with a 4-7 risk score and a high-risk assessment to a customer with 8-10 risk score.

Members of staff may take into account any applicable mitigation reasons set out in the table above, in which case the reasons for the mitigation are recorded. The risk assessment may be revised on the basis of these mitigations subject to the consideration that a risk may never be assessed as low where:

- i. the client is non-face-to-face (save for those instances detailed in the section entitled “Simplified Due Diligence” a) or b))
- ii. the client is a PEP
- iii. the client is from or is active in a high-risk jurisdiction

Annex III – Customer Due Diligence

The Company has established systematic procedures for identifying an applicant for business and ensuring that such identity is verified on the basis of documents, data or information obtained from a reliable and independent source.

Persons subject to Identification and Verification

For the purposes of the gaming services provided the follow legal and/or natural persons shall be subject to identification and verification procedures as stipulated below.

- i. The Player being the natural person who is registered with the Company to which online gambling services are provided by the Company;
- ii. A company or legal entity which is considered to be an intermediary of the Company to which online gambling services are provided by the Company;
- iii. The Ultimate Beneficial Owners of a Company or legal entity which is considered to be an intermediary of the Company;
- iv. The Directors of a Company or legal entity which is considered to be an intermediary of the Company;

For the purposes of the above that the “**ultimate beneficial owner**” of a body corporate or a body of persons includes all natural persons who ultimately own or control, whether through direct or indirect ownership or control, 25% or more of the shares or voting rights in the Company or legal entity in relation to which services are or will be provided.

Provided that natural persons who ultimately own or control a company that is listed on a regulated market which is subject to disclosure requirements consistent with Community legislation or equivalent international standards shall be excluded from verification

Initial
ME

DS

requirements.

Provided further that in the case of a trust where beneficiaries have not been determined, due diligence will be carried out on any class of persons in whose main interest the trust is set up.

For the purposes of the above that the “**beneficial owner**” of a body corporate or a body of persons includes all legal persons who own or control, whether through direct or indirect ownership or control, 25% or more of the shares or voting rights in the Company or legal entity in relation to which services are or will be provided,

Provided that companies that are listed on a regulated market or otherwise subject to financial business regulation which are subject to disclosure requirements consistent with Community legislation or equivalent international standards shall be excluded from verification requirements. In such a case Simplified Due Diligence should be followed for Client On-boarding.

Provided that for Directors, the Company shall only be required to identify such persons and hence, notwithstanding anything to the contrary, no verification shall be required to be collected.

Organogram

In order to be able to identify each of the persons subject to identification and verification as part of the on-boarding process, the applicant for business is to provide an up-to-date organogram to the Company which is to be signed by an authorized official of the applicant, both at on-boarding and each time that there is a significant change in ownership.

Due Diligence for Natural Persons

Where the persons subject to identification and verification are natural persons, the following information shall be obtained in all cases in relation to identification and verification:

OPTION A:

1. Verification of Details - one of the following:
 - 1.1. a valid unexpired passport; or
 - 1.2. a valid unexpired national or other government-issued identity card; or
 - 1.3. a valid unexpired driving license.
2. Verification of Residential Address - one of the following not older than six (6) months:
 - 2.1. a recent statement from a recognized credit institution;
 - 2.2. a recent utility bill;
 - 2.3. correspondence from a central or local government authority, department or agency;
 - 2.4. any government-issued document where a clear indication of residential address is provided; or
 - 2.5. any other document as may be issued by the FIU.

In addition to the above, one of the following Options shall be satisfied for the purposes of

Initial
ME

DS

Enhanced Due Diligence where the Customer's risk has been assessed as '**Medium Risk**' and two of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Customer's risk has been assessed as '**High Risk**' as follows:

OPTION 1: One of the following

1. a professional reference (warranted lawyer or auditor)
2. a bank reference
3. an additional recent statement from a recognized credit institution;
4. an additional recent utility bill;
5. correspondence from a central or local government authority, department or agency;
6. any government-issued document where a clear indication of residential address is provided; or
7. any other document as may be issued by the FIU.

OPTION 2:

1. *The first payment be made from a bank set up in the EU or of a reputable jurisdiction with similar standards of banking regulation. For the purposes of this option 'bank' may also include financial institution, payment institution or electronic money institution.*

OPTION 3:

1. *Determination of source of wealth and source of funds signed by a recognized accountant/auditor.*

OPTION 4:

1. *Police conduct certificate*

OPTION 5:

Require that the documentation provided in OPTION A.2 and A.3 above is certified by a legal professional, accountancy professional, notary, person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction. Such certification should be evidenced by a written statement stating that:

- the document is a true copy of the original document;
- the document has been seen and verified by the certifier; and
- the photo is a true likeness of the applicant for business or the beneficial owner, as the case may be.

The certifier must sign and date the copy document (indicating his name clearly) and clearly indicate his profession, designation or capacity on it and provide his contact details.

Provided that in all cases where the applicant, beneficiary owner or the ultimate beneficial owner is a PEP, Temple Holdings N.V. will proceed to end the relative business relationship.

Initial
ME

DS

Due Diligence for Legal Persons

Part A

Where the persons subject to identification and verification are legal persons the following information shall be obtained in all cases in relation to identification and verification:

- a) to identify the following:
 - i) the legal person's official full name;
 - ii) the legal person's registration number (if applicable);
 - iii) the legal person's date of incorporation or registration; and
 - iv) the legal person's registered address or principal place of business.

- b) To verify the information and legal status mentioned under Part A(a), the most recently dated version of any of the following documents must be obtained:
 - i) Memorandum and Articles of Association; or
 - ii) Certificate of Incorporation; or
 - iii) Signed declaration by an authorized official of the applicant for business; or
 - iv) Company registry search, which includes confirmation that the private company has not been, and is not in the process of being dissolved, struck off, wound up or terminated; or
 - v) Latest annual return; or
 - vi) Other statutory document.

In relation to the above, the staff member must view the original document, a certified copy of the original or a downloaded copy from the official registry website. Certification should be carried out by the company secretary, a director or an officer occupying an equivalent position or by the Registrar of Companies or a person occupying an equivalent position in a foreign jurisdiction.

Alternatively, certification may be carried out by a legal professional, accountancy professional, notary, person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction.

The certifier must sign and date the copy document (indicating his name clearly) and clearly indicate his profession, designation or capacity on it and provide his contact details.

The certified copy of the original or the copy downloaded from the official registry website shall be retained by Temple Holdings N.V. Where an original document is viewed, Temple Holdings N.V. shall keep a true copy of the document, signed and dated by an officer of the subject person, on file.

Alternatively, identification and verification may be carried out by obtaining one or more additional (different) documents from amongst the list provided in Part A (b) above which verify the information obtained through the first set of documentation provided.

Initial
MC

DS

In addition to the above, one of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Customer's risk has been assessed as '**Medium Risk**' and two of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Customer's risk has been assessed as '**High Risk**' as follows:

OPTION I:

1. Latest audited financial statements; provided that in case of Enhanced Due Diligence, this shall only be required if allowed by the jurisdiction of the applicant for business.

OPTION II:

1. The first payment be made from a bank set up in the EU or in any other jurisdiction with similar standards of banking regulation. For the purposes of this option 'bank' may also include financial institution, payment institution or electronic money institution.

OPTION III:

1. Certificate of good standing or a certificate of incumbency, not older than six (6) months.

OPTION IV:

1. A professional reference signed and duly dated by a legal professional, accountancy professional or notary.

Part B

Post identification and verification of the Legal Person, the Company shall also identify all the directors. This shall be done by either of the following:

- i) referring to the list of directors contained in the most recent version of the Memorandum and Articles of Association; or
- ii) by performing a company registry search provided that the officers of the company are listed therein; or
- iii) by obtaining a copy of the directors' register of the company.

Part C

Upon the identification of the shareholders and Ultimate Beneficiary Owners' details as a result of the Organogram and documentation provided as mentioned above, the staff member shall perform and record the Due Diligence provided for natural persons in respect of such Ultimate Beneficiary Owners with particular regard to non-face-to-face procedures if required:

Provided that should the applicant's operations be regarded as high risk, shareholders having between 10% but less than 25% of the control in the applicant, may be required to provide for

Initial
ME

DS

identification details including but not limited to First Name, Last Name and Date of Birth.

In instances where the documentation provided under Part A(b) does not identify the shareholders and the Ultimate Beneficiary Owners, the applicant for business has to supply any of the following documents:

- i) Latest share register; or
- ii) Signed declaration by an authorized representative of the applicant for business, which declaration should include sufficient details to enable the subject person to identify the shareholders and the Ultimate Beneficiary Owners.

For avoidance of doubt, no proof of address will be requested of shareholders holding an interest between 10%, but less than 25%.

Languages

All documents are to be provided in English (or any other language which any official of the Company understands). Certified translations are to be translated of documents in other languages.

Client Terms and Conditions

The Client Terms and Conditions includes a declaration by an authorized representative of the applicant for business as to whether they have:

- a) ever been convicted of an offence (other than a minor traffic offence);
- b) ever been adjudged bankrupt;
- c) ever been the subject of an investigation by a government, professional or other regulatory body;
- d) ever been a director, shareholder, officer or manager of a business entity which has been the subject of an investigation as aforesaid
- e) ever been a director, shareholder, officer or manager of a business entity which has been adjudged bankrupt compulsorily would up or has made any compromise or arrangement where its creditors or has otherwise ceased trading in circumstances where its creditors did not receive or have not yet received full settlement of their claims; and
- f) unless otherwise disclosed in the terms and conditions, ever had or currently has any direct or indirect beneficial interest in or whether he ever was or currently is a director of any other company registered in Curaçao.

Customer Risk Assessment

Each customer is subject to a risk assessment and subsequently rated as Low Risk, Medium Risk or High Risk as set out in Annex II above. For the purposes of such assessments additional information may be required from the customer.

Face-To-Face Transactions or Clients

In all instances of face-to-face onboarding, provided that the applicant does not provide certified true hardcopies or the originals of the documentations required as per the abovementioned procedures, the Company representative is to view the original document,

Initial
MC

DS
[Signature]

make a hard copy of such document (printed scan/photograph etc.) and certify that this is a true copy of the original seen by him, while duly signing the document including the relevant date.

All instances of face-to-face clients will require any one of the following:

- a) Include an email on file confirming that a face-to-face meeting with the applicant for business duly occurred prior to onboarding;
- b) A certified true copy in original by a Temple Holdings N.V.'s representative of an identification document of the applicant for business' representative, provided that such document was copied (scanned, photographed etc.) by a Company's representative himself; or
- c) Minutes of the meeting with the applicant for business' representative, signed and duly dated by the Company representative.

Timing of Due Diligence

Each client shall provide a copy of all documentation in order to assess that all the documentation is in order upon the first withdrawal and/or upon the sum of Naf 4,000 (Eur 2,000) with accumulative withdrawal threshold reached by the player.

In some instances, a corporate client (intermediary) may select to sign the Services Agreement prior to the carrying out of on-boarding to provide a commitment to eventual onboarding. In this case, no services are permitted, and no services shall be provided to the client and no transactions entered into prior to the carrying out of all due diligence procedures and prior to on-boarding.

In the event that due diligence documentation is not provided within thirty (30) days from the initial request by the Company or it otherwise becomes obvious that the client is not able to satisfy due diligence requirements, the Service Agreement or player registration shall be terminated. The AML/CFT Compliance Officer will consider the appropriateness of filing an UTR.

Initial


DS


Annex IV – Client Acceptance Policy

The Companies or intermediary of the Company policy for acceptance of customers takes into consideration the Risk Assessment and Mitigation measures as well as the Risk Factors indicated in Annex II above.

Client Acceptance

The Company or an intermediary of the Company shall not accept the following clients:

- i. Clients that fail the relevant due diligence identification and verification controls set out in Annex III above;
- ii. Clients who themselves or their ultimate beneficial owners are excluded customers listed below;
- iii. Clients who have in the past been reasonably associated or involved in criminal activities or other illegal activities may result from searches on the clients, beneficial owners and on any other person in relation to whom due diligence is carried out.

Excluded Activities

The Company or its intermediaries shall not accept the following types of business activities for any provision of services:

- i. Trading in Arms
- ii. Supplying Technology or Parts Connected with Defense
- iii. Providing Military Security Services
- iv. Clients resident in jurisdictions where the Company - or its affiliated Group Companies with whom service agreements are in place - are not authorized to provide gaming services.

Excluded Individuals

The Company or its intermediaries shall not accept the following persons:

- i. Sanctioned Individuals and/or entities;
- ii. Politically Exposed Persons (PEPs);
- iii. Entities with bearer shares;
- iv. Entities where UBOs cannot be identified;
- v. Persons who seek to set up a business relationship or conduct an occasional transaction in the name of third parties under an anonymous name or nickname;
- vi. Customers having underlying customers

Risk-Based Approach for Accepting Clients

On the basis of the risk approach highlighted in Section 3 of the AML Policy and Annex II above, risk factors are taken into account to determine the risk of each customer (low, medium or high). Different levels of Enhanced Due Diligence are applied in the event of Medium or High-risk assessments.

The manner in which the assessment is carried out is highlighted in Annex II above.

Initial
ME

DS

Annex V – Internal UTR Form

Internal UTR Form Template

The UTR should be a prompt report and escalated to the FIU as soon as practically possible.

(Please send the Internal UTRs to the AML/CFT Compliance Officer and cc the Deputy if exist)

A record of this UTR together with all related documents will be kept by the AML/CFT Compliance Officer for at least five (5) years.

Reporter's details (this section is to be completed by the Reporter)	
Reporter's name:	
Reporter's email:	
Date:	
Department:	

Individual subject(s) of the UTR (this section is to be completed by the Reporter)	
Customer's user ID/username/brand:	
Relationship start & end date:	
Customer's full name:	
Customer's residential address:	
Customer's date of birth:	
Customer's phone number(s):	
Customer's email address:	
Customer's gender:	
Customer's nationality:	
Linked account(s):	
What is the reason for reporting?	
Multiple Accounts?	Y/N
Use of Multiple IP Address via Proxies/VPNs to Mask Location and/or Identity?	Y/N
Suspected Account Hijacking?	Y/N
Unusual Gaming / Account Activity?	Y/N
Bonus Abuse?	Y/N
Fraudulent Refund Request?	Y/N
Non-Compliance with Requests?	Y/N
Other (please specify)	
What evidence is supporting your suspicion? (Please add sources & links such as: transaction records, chat logs, email correspondence, account activity logs, screenshots, etc.).	

Initial
MC

DS
[Signature]

Aggregate lifetime deposits (across brands):	
Aggregate lifetime withdrawals (across brands):	
Balance (including pending WDs) in account at UTR reporting date (across brands):	
AML details (this section is to be completed by the Reporter)	
ID Reference Number:	
ID Expiry Date:	
Known occupation:	
CDD / EDD Status:	
Status of business relationship:	
Services utilized:	
Reference nr. if linked to a previous UTR:	

Activity Information (this section is to be completed by the Reporter)
Provide a comprehensive description of the unusual activity, including dates, times, and any relevant transactions or behaviors observed. Please also provide an overall total of deposit/withdrawal amount for each payment method, including the first and last date of each payment method used. <i>It may be easier to export this as an excel document and attach.</i>

Supporting documentation attached (this section is to be completed by the Reporter) <i>When you escalate the internal UTR please attach in the email: ID, Proof of address documents, deposit history (excel sheet), withdrawal history (excel sheet), login history (IP address on excel sheet), chat logs, email correspondence, account activity logs, screenshots, etc.</i>	
Customer Due Diligence Documents (ID / UB):	Customer Notes:
List the IP addresses customer used to log on:	Customer Communications Logs:
Value and volume of withdrawals and deposits:	Payment Gateway Information related to customer:

Initial
MC

DS
[Signature]

Timeline of the Unusual Activity (this section is to be completed by the AML/CFT Compliance Officer)

(The timeline should be detailed and sufficiently clear that someone not familiar with the activity or Company would understand it. Please avoid jargons and acronyms)

xx/xx/xxxx – Customer opened his/her xx account

xx/xx/xxxx – We verified ID, Proof of address, etc.

xx/xx/xxxx – We found a negative adverse media regarding our player *(include link if available, date and a short summary about the article)*

xx/xx/xxxx – Account was closed.

xx/xx/xxxx – An internal UTR was considered.

The information or other matter which gives the grounds for your knowledge, suspicion, or belief:

- Negative adverse media have found;
- Possible problem gambling signs;
- No cooperation with our Due Diligence Documentation / Source of Wealth request.
- No cooperation with our Customer Support / Risk, Payments & Fraud Team.

AML/CFT Compliance Officer Determination (this section is to be completed by the AML/CFT Compliance Officer)

3. Did we find positive info online on the player that would discharge our concerns?

4. Did we find any negative info found online or in the account history, data, behavior, documents etc, that would mean we clearly need to report?

Should the answers to be no for both of these, we must consider:

- The country is x AML risk according to FATF,
- Payment method is x risk (visa, bank, etc.),
- spend is x risk.

I suggest we file this as a UTR, but that will depend on the answers above.

Initial
ME

DS

Annex VI – Business Risk Assessment

In accordance with regulatory expectations set forth by the Curaçao Gaming Authority, the Company has conducted a comprehensive Business Risk Assessment addressing all relevant operational, compliance, and financial risk factors.

Due to the scope, length, and level of detail required to meet these regulatory standards, the full Business Risk Assessment has been compiled as a standalone document. This allows for a thorough review of identified risks, control measures, and the Company's ongoing risk mitigation strategies.

In short, the Business Risk Assessment of the Company includes:

- an introduction of Temple Holdings N.V.;
- identification and scoring of inherent risks;
- determination of risk appetite;
- analysis of AML/CFT controls;
- determination of residual risks;
- remediation plan;
- conclusion; and
- an appendix for weighing and scoring.

For complete information, please refer to the separate document titled "Business Risk Assessment – Temple Holdings N.V.".

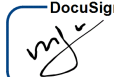
Initial


DS


Annex VII – Abbreviations

AML	Anti-Money Laundering
AML Regulation	Regulations Concerning Anti-Money Laundering and Countering Terrorism Financing
CMP	Compliance Monitoring Program
CFT	Combating Funding of Terrorism
EU	European Union
KYC	Know Your Customer
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
TF	Terrorist Financing
ML	Money Laundering
PEP	Politically Exposed Person
RBA	Risk Based Approach
UTR	Unusual Transaction Report

Annex VIII – Signatory page

DocuSigned by:

16/05/2025
215940689FEB429...

Starkeast Management B.V., Managing Director
By: Menno Jordaan, as director of Starkeast Management B.V.

Signed by:

16/05/2025
C844330A35F54B6...

Mark Cauchi
Key Compliance / MLRO

Initial


DS


Temple Holdings N.V.

Business Risk Assessment

CONFIDENTIALITY STATEMENT

This is a confidential document for Temple Holdings N.V. It contains confidential and/or proprietary information that may not be disclosed or discussed with anyone outside the organization without written approval of Temple Holdings N.V.

Initial


DS


Document Version Control

Version	Date	Security class	Author	Purpose
1.0	26/08/2024	Confidential	Temple Holdings N.V.	Creation of this document

Initial


DS


Table of Contents

1.	<i>Introduction</i>	4
1.1	The Company.....	4
1.2	Risk characteristics	4
1.3	EU Supranational Risk Assessment & National Risk Assessment	5
1.4	Methodology	7
2.	<i>Identification and scoring of inherent risk</i>	9
2.1	Inherent risk – Games.....	12
2.2	Inherent risk – Payment methods	14
2.3	Inherent risk – Jurisdictions and players	16
2.4	Inherent risk – Delivery channels	20
2.5	Total inherent risk	21
3.	<i>Determination of risk appetite</i>	22
4.	<i>Analysis of AML/CFT controls</i>	23
4.1	Controls – Games	23
4.2	Controls – Payment methods	26
4.3	Controls – Customer Due Diligence.....	28
4.4	Controls – Delivery channels	31
4.5	Controls – Risk assessment.....	32
4.6	Controls – Transaction monitoring and reporting	33
4.7	Controls – Internal audit.....	34
4.8	Controls – Record keeping.....	35
4.9	Controls – Training and HR.....	36
4.10	Controls – MLRO and compliance	37
4.11	Controls – Governance	38
4.12	Controls – Outsourcing	39
4.13	Overall controls	40
5.	<i>Determination of residual risk</i>	41
5.1	Residual risk – Games	42
5.2	Residual risk – Payment methods.....	42
5.3	Residual risk – Jurisdictions and players.....	42
5.4	Residual risk – Delivery channels.....	43
5.5	Total residual risk	43
6.	<i>Remediation plan</i>	44
7.	<i>Conclusion</i>	46
	<i>Appendix I – Business Risk Assessment excel sheet (scoring and weighing)</i>	46
	<i>Board of Directors signature page</i>	47

Initial
MC

DS
[Signature]

1. Introduction

1.1 The Company

Temple Holdings N.V. (hereinafter referred to as “Temple Holdings” or as “the Company”) is registered in Curaçao with registration number 159511 and registered address at Kaya W.F.G. (Jombi) Mensing 24 Unit A, Willemstad, Curaçao. Temple Holdings is a B2C remote gaming company, Curaçao licence number is OGL/2024/1581/0803 and operating through the websites under the license

1.2 Risk characteristics

The Company’s business activity is that of a remote gaming provider offering gaming services – casino, sportsbook and “virtuals” services. This activity constitutes a “relevant activity” in terms of Curaçao’s GCA regulations.

According to the National Risk Assessment (hereinafter referred to as “NRA”) of Curaçao, the overall Money Laundering and Financing of Terrorism (hereinafter “ML/FT”) risk for online gambling was rated as **High**, driven by the following components:

- Curaçao is among the top 3 countries where the most servers of online gambling sites are located;
- the fact that online gambling is a cross-border activity without any real borders makes this sector even more attractive to money launderers, because of the opportunities offered to misuse the legislative, administrative, judicial differences between countries to continue criminal activities regardless of actions taken by governments;
- the vulnerability of this sector in Curaçao is exacerbated by the practice of the previous sub-licensing without any regulatory oversight. Transparency was lacking and the sector was de-risked many years ago. The inherent vulnerability as well as the final vulnerability are assessed as HIGH

“Online gambling is inherently vulnerable to ML due to the high number of customers, high volume of transactions, the nonface-to-face nature of the business, the high percentage of non-resident customers and the use of prepaid cards that are not linked to a bank account. This is further evidenced by the high number of UTRs received. Certain remote gaming

Initial
MC

DS
[Signature]

activities are more vulnerable than others. For instance, P2P and sports betting are more exposed than bingo or lotteries as they involve a transfer of value or predictable, low losses.”

The available statistical data and evidence led the Curaçao authorities to take a conservative view of the country’s FT threats hence resulting in a risk rating of High. The national threat is two-fold – stemming from the risk of terrorism itself and the risk of terrorism financing.

In the sectoral ML/FT vulnerability assessment, the NRA has identified online gambling as having an inherent risk rating as High. The overall level of controls in the sector was indicated as being Low, resulting in a residual risk rating of High.

1.3 EU Supranational Risk Assessment & National Risk Assessment

On the 24th of July 2019, the European Commission published its revised Supranational Risk Assessment Report (hereinafter referred to as “SNRA”) as required by the 4th Anti-money Laundering Directive. The Commission assessed the vulnerability of financial products and services to risks of money laundering and terrorist financing. This risk analysis is conceived as a key tool to identify, analyse and address money laundering and terrorist financing risks in the EU. It aims at providing a comprehensive mapping of risks on all relevant areas, as well as recommendations to Member States, European Supervisory Authorities and obliged entities to mitigate these risks. This risk analysis supports Member States and obliged entities when carrying out their respective risk assessments.

The SNRA has shown that *“For **online gambling** there is a high-risk exposure due to very large numbers of transaction- flows and the lack of face-to-face interaction. Although casinos present inherently high-risk exposure, their inclusion in the anti-money laundering/countering the financing of terrorism framework since 2005 has had a mitigating effect.”*

The Fifth Money Laundering Directive (5AMLD) came into force on the 10th of January 2020. Building on the regulatory regime applied under its predecessor, the Fourth Money Laundering Directive (4AMLD). 5AMLD reinforces the European Union’s AML/CFT regime to address a number of emergent and ongoing issues. The impact of 5AMLD is far-reaching. Key changes from the 5AMLD – which are relevant to our business – have been listed below:

- makes a significant new legislative step in the treatment of virtual currencies,
- sets a lower limit of EUR 150 for prepaid card transactions,
- companies that do business with customers from high-risk third countries are, under 5AMLD, required to perform enhanced due diligence measures,
- 5AMLD requires EU member states to compile and publicly release a functional PEP list made up of prominent politically exposed public functions.

The 4th and 5th Anti Money Laundering Directive require that obliged entities take into account the findings of any applicable national risk assessments together with the EU Supranational Risk Assessment (SNRA) when determining the inherent risk of a business. Therefore, the results of the Curaçao National Risk Assessment (NRA) and the SNRA were considered and factored into the assessment. The SNRA has specifically identified that online gambling operators are exposed to a high risk of ML/FT due to the huge volumes of transactions passing through the operator on a daily basis, the ability of players to use anonymous means of payment and the non-face-to-face element discussed above.

The 6th AMLD is not out yet, although there was the notion that there was. The Directive (EU)2018/1673 was an enhancement of the 5th AMLD - Combatting ML by Criminal Law – the 6th AMLD is in the pipeline, probably will be a regulation not a directive. There is the new AMLA brewing.

Under the current rules, only individuals can be punished for the act of money laundering; however, 6AMLD will extend criminal liability to allow for the punishment of legal persons, such as companies or partnerships. The new rules mean that a legal person will be considered culpable for the crime of money laundering if it is established that they failed to prevent a “directing mind” from within the company from carrying out the illegal activity. Practically, the new rules will place AML/CFT responsibility on management employees along with employees acting separately.

The extension of criminal liability in this context is intended to hold larger companies to account in the global effort to combat money laundering. The move will allow financial authorities to better target organizations that do not implement AML/CFT effectively. Punishments for legal persons may range from a temporary ban on operations or judicial supervision to permanent closure.

The Company developed an understanding of the adjusted scope that 6AMLD brought to it, including new predicate offenses that must be monitored and the new risk environment in which they will be operating. In addition to managing their AML resources and training compliance staff, the Company reviewed their technology deployment in order to ensure that they have the capability to meet their new transaction monitoring and screening obligations.

Initial


DS


1.4 Methodology

Establishing a clear understanding of the money laundering and terrorist financing (ML/FT) risk that the Company is exposed to is an essential component for it to develop and implement an effective anti-money laundering / counter-terrorist financing (AML/CFT) framework. The company-wide risk assessment that has been carried out provides a detailed analysis of the AML/CFT risk associated with the Company's products, the payment methods it accepts and its customer base. Other qualitative and quantitative factors such as the NOIS and NORUT, Sanctions National Ordinance and Kingdom Sanction Act for the online gambling sector with all relevant regulations and the conclusions of the EU Supranational Risk Assessment have also been considered.

It is important to point out that the Company has made significant improvements to bring its processes and procedures in line with its obligations. Although there is always room for improvement, the Company has implemented several changes and tools, which shows a great commitment.

In the process of carrying out the business risk assessment, the below mentioned critical steps were undertaken. These steps were carried out in the course of different project phases, as described in parts 2 to 6 of this document.

STEP 1: Identification and analysis of the inherent risk exposure of Temple Holdings across a wide range of categories such as its customers, games, geographical areas, delivery methods and payment methods.

STEP 2: The determination of the level of risk that the Company considers acceptable.

STEP 3: Identification, analysis and testing of the AML/CFT controls currently in place to mitigate the inherent risk within the business undertaken by Temple Holdings N.V.

STEP 4: Determination and quantification of the residual risk.

STEP 5: A remediation plan outlining the steps that will be taken to reduce the level of risk and retain it within the risk appetite established by the Company's directors, also to strengthen controls that the Company has in place already.

Appendix I. is showing the weighing and scoring for all of the tables (related to inherent risks, residual risks and controls) below, which are included in this BRA. Certain questions have been asked related to each field in order to identify any risks/gaps and also questions were asked regarding how effective the controls are within the Company for the said field. Different answers will give different scores, which will provide a final score for every field (*for example: Risk Factors – Table Games = 0*).

Also, the probability, the impact and the importance of each field is visible in the Appendix which derive from Table 1, Table 2 and Table 3.

Explanation for the description of score (satisfactory, needs improvement and deficient)

Satisfactory: this score has been used when a field is fulfilling expectations or needs; it is acceptable from a regulatory point of view, though not outstanding or perfect.

Needs improvement: this score was given when the company already made efforts in order to implement improvements on a specific field, however it might be not up to industry standard or fulfil our regulatory obligation 100%.

Deficient: lacking in some necessary quality or element. This can mean we are not compliant, or we are in a potential breach from a regulatory point of view.

Initial


DS


2. Identification and scoring of inherent risk

With the participation of company employees and senior management we aimed at obtaining a broader and deeper understanding of the inherent risks to which the Company is exposed. A detailed analysis of the Company's jurisdictional risk was carried out, the risk emanating from the payment methods used and the level of inherent risk posed by the different games offered by the Company, with a detailed examination being undertaken on all categories of games.

Participants in this process included the Senior Management of the Company.

Each risk factor was assessed separately, and its risk score calculated on the basis of the likelihood of the occurrence of the risk event and the impact that such risk event might have on the Company's operations. The probability of a risk factor occurring is a combination of threat and vulnerability, whilst impact can be defined as the loss and damage, both financially and reputationally, that would be suffered if such risk were to materialize.

Likelihood	Description
Rare	A very remote chance of happening i.e. the risk will only occur in exceptional circumstances
Unlikely	There is a small chance of the risk happening
Moderate	Neither likely nor unlikely to happen, but there is a reasonable chance of the risk occurring
Likely	The risk is likely to happen
Very likely	A very high chance of happening (almost expected) i.e. the risk is most likely to occur

Table 1: Likelihood – Description

Impact	Definition	Comments
Trivial	A ML/FT breach will have a trivial impact or no impact at all if the risk were to occur	• No regulatory enforcement actions • No adverse national media coverage • Isolated possible customer complaints
Minor	A ML/FT breach will have a minor impact if it were to occur i.e. impact will be almost insignificant	• No regulatory enforcement other than a possible warning or reprimand • Isolated adverse national media coverage • Increasing possibility of customer complaints
Moderate	A ML/FT breach will have a moderate impact if it were to occur i.e. impact will be potentially significant and noticeable, but can be handled with the resources that are currently available	• Formal private regulatory warnings or minor financial penalties • Short term adverse national media coverage • Contained increase in customer erosion
Major	A ML/FT breach will have a major impact if it were to occur i.e. business reputation and income will be seriously impacted and will present challenges for the business	• Significant suspension of business or license approvals and/or pecuniary regulatory measures • Sustained adverse national media coverage • Significant increase in customer erosion
Extreme	A ML/FT breach will have an extreme impact if it were to occur i.e. business reputation and income effectively being threatened	• Criminal or civil actions against the Company or its Directors • Sustained adverse national / international media coverage possibly coupled with regulatory intervention • Suspension of business license approvals and/or significant regulatory fines • Possible withdrawal of license to operate

Table 2: Impact – Definition

Initial
MC

DS
[Signature]

The heatmap shown in Table 3 below outlines the level of importance assigned to each factor in relation to probability and impact:

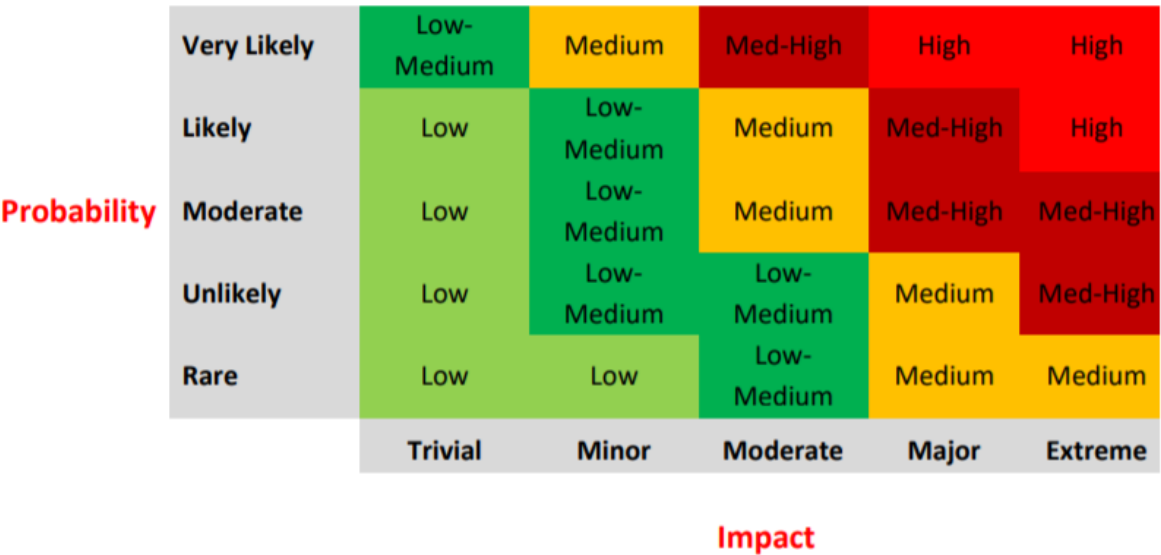


Table 3: Importance level – Risk Heatmap

The attributable level of importance was then given a score range as categorised in Table 4 below. Therefore, in those cases where a risk factor was assessed as having a high or likely probability of increasing ML/FT risk and a resultant major impact on the Company would ensure if the risk materialized, through the use of the matrix in Table 1, the level of importance of that risk factor would be Medium-High. A score would then be assigned to this importance level according to the ranges shown in Table 2, resulting in a score range of between 63 and 83 points for a Medium-High level of importance.

Importance Level	Score Range
High	84 – 100
Medium – High	63 – 83
Medium	42 – 62
Low – Medium	21 – 41
Low	0 – 20

Table 4: Risk score for Level of importance

The full list of scores and weighting applied are presented in Appendix I. A breakdown of the level of risk identified per category is provided in the paragraphs hereunder.

2.1 Inherent risk – Games

One of the main risk categories that is considered in the risk assessment is the risk derived from the products offered by the Company. These being:

- Casino games (including Table games, Live casino games and Slots);
- Sports betting; and
- Virtuals.

When identifying and assessing this category of risk, all the games provided by the Company were taken into consideration. The following tables provide the risk scoring range for games, as well as the risk factors identified and the inherent risk rating per game type:

Score Range Games	Risk Rating
0 – 80	Low
81 – 160	Low – Medium
161 – 240	Medium
241 – 320	Medium – High
321 – 400	High

Table 5: Games – Inherent risk score range

Casino games		
Risk factors	Answer	Score
Is there a possibility of chip dumping?	No	0
Is it possible for players to collude?	All games are RNG-based; possibility of collusion is so remote that it has been excluded. However, in live casino games it is possible with the involvement of casino employees or game providers	81
Is placing safe bets possible?	No	0
Is there an element of skill?	No	0
Table games – Risk rating	Low-Medium	81

Table 6: Casino games – Inherent risk rating

Initial
MC

DS
[Signature]

Sports betting		
Risk factors	Answer	Score
Is there a possibility of chip dumping?	No	0
Is it possible for players to collude?	No	0
Is placing safe bets possible?	Sometimes	81
Is there an element of skill?	Sometimes	81
Table games – Risk rating	Medium	162

Table 7: Sports betting – Inherent risk rating

Virtuals		
Risk factors	Answer	Score
Is there a possibility of chip dumping?	No	0
Is it possible for players to collude?	No	0
Is placing safe bets possible?	No	0
Is there an element of skill?	Yes	81
Table games – Risk rating	Low – Medium	81

Table 8: Virtuals – Inherent risk rating

The following tables provide the overall risk range for the scoring of games and the overall inherent risk rating in relation to all the games:

Overall Score Range Games	Risk Rating
0 – 240	Low
241 – 480	Low – Medium
481 – 720	Medium
721 – 960	Medium – High
961 – 1200	High

Table 9: Overall inherent risk score range for Games

Games	Low risk	Low-Medium risk	Medium risk	Medium-High risk	High risk
Casino games		81			
Sports betting			162		
Virtuals		81			
TOTAL	SCORE: 324 = RISK: Low-Medium				

Table 10: Overall inherent risk rating for Games

2.2 Inherent risk – Payment methods

Another risk category that was considered in the risk assessment is the risk derived from the payment methods used by Temple Holdings N.V. Each payment method offered by the Company has been assessed and examined in detail to determine the degree to which the specific characteristics of the payment method render users vulnerable to ML/FT threats.

The payment methods accepted by the Company are the following and their respective risk assessment is provided in the tables below:

- Crypto payment via Coinspaid

Score Range	Risk Rating
0 – 100	Low
101 – 200	Low – Medium
201 – 300	Medium
301 – 400	Medium – High
401 – 500	High

Table 11: Payment methods – Inherent risk score range

Crypto payments		
Risk factors	Answer	Score
Is there a possibility of anonymity?	Yes	100
Is it possible to fund it anonymously?	Yes	100
Can it be reloaded?	No	0
Can a closed-loop policy be applied?	No	100
Are they issued by a licensed financial institution in a reputable jurisdiction?	Yes, but the AML obligations are less rigorous	81
Risk	Medium – High	381

Table 12: Crypto payments – Inherent risk rating

The following tables provide the overall risk scoring range for payment methods and the overall inherent risk rating in relation to all the payment methods:

Overall Score Range Games	Risk Rating
0 – 100	Low
101 – 200	Low – Medium
201 – 300	Medium
301 – 400	Medium – High
401 – 500	High

Table 13: Overall inherent risk scoring range for Payment methods

Payment methods	Low risk	Low-Medium risk	Medium risk	Medium-High risk	High risk
Crypto payments				381	
TOTAL	SCORE: 381 = RISK: Medium-High				

Table 14: Overall inherent risk rating for Payment methods

2.3 Inherent risk – Jurisdictions and players

The company's customer base cannot be reviewed in detail to determine which customer risk factors may increase the ML/FT risk of the Company as the Company has not yet launched. Subsequently, the following categories were used to stratify the customer base and identify aspects of customer risk:

PEP status, High value depositing players (VIP players), Customers with adverse news hit / sanctions hit, Customers who deposited or withdrew without gambling activity, High risk customers associated with high-risk industry, High-risk players and High-risk payment methods used.

The assessment also included a review of the geographic locations of the customer base that the Company is planning to target, as this factor is a core component of any inherent risk assessment. The Company has, in fact, evaluated the specific risks associated with doing business in, opening and servicing, offering products and services to and/or facilitating transactions involving certain geographic locations.

Each player type will be assigned with a risk score to determine the ML/FT risk each category of players poses to the Company. The risk scoring range for player jurisdictions and different player types, as well as the risk factors identified and the risk ratings per jurisdiction and player types, is provided in the tables below:

Score Range Jurisdiction	Risk Rating
0 – 30	Low
31 – 60	Low – Medium
61 – 90	Medium
91 – 120	Medium – High
121 – 145	High

Table 15: Player Jurisdiction – Inherent risk score range

Player Jurisdictions		
Risk factors	Answer	Score
What % of players are resident in medium risk jurisdictions?	N/A	0
What % of players are resident in high-risk jurisdictions?	N/A	0
Player Jurisdiction Risk	N/A	0

Initial
MC

DS
[Signature]

Table 16: Player Jurisdiction – Inherent risk rating

Score Range PEPs	Risk Rating
0 – 36	Low
37 – 72	Low – Medium
73 – 108	Medium
109 – 144	Medium – High
145 – 183	High

Table 17: PEPs – Inherent risk score range

Politically Exposed Persons (PEPs)		
Risk factors	Answer	Score
What % of players are PEPs?	N/A	0
What % of players are resident in high-risk jurisdictions?	N/A	0
PEP Risk	N/A	0

Table 18: PEPs – Inherent risk rating

Score Range High Depositors	Risk Rating
0 – 52	Low
53 – 105	Low – Medium
106 – 157	Medium
158 – 210	Medium – High
211 – 262	High

Table 19: High depositors – Inherent risk score range

High Depositors		
Risk factors	Answer	Score
What % of players have deposited (at least once) more than Euro 2,000 in one day?	N/A	0
What % of players have deposited (at least once) more than Euro 10,000 in one month?	N/A	0
What % of players have deposited (at least once) more than Euro 30,000 in a lifetime?	N/A	0
High Depositors Risk		

Initial
MC

DS
[Signature]

Table 20: High depositors – Inherent risk rating

Score Range	Risk Rating
High Risk Players	
0 – 100	Low
101 – 200	Low – Medium
201 – 300	Medium
301 – 400	Medium – High
401 – 500	High

Table 21: High risk players – Inherent risk score range

High Risk Players based on Payment Methods		
Risk factors	Answer	Score
What % of players are considered to be high risk?	N/A	0
What % of total deposits are done through cards including prepaid cards?	N/A	0
What % of total deposits are done through e-wallets?	N/A	0
What % of total deposits are done through paysafe cards and vouchers?	N/A	0
What % of total deposits are done through crypto payments?	N/A	0
High Risk Players Risk	N/A	0

Table 22: High risk players – Inherent risk rating

Initial
MC

DS
[Signature]

The following tables provide the overall risk scoring range for players and the overall inherent risk rating in relation to all player types:

Overall Score Range Jurisdictions & Players	Risk Rating
0 – 218	Low
219 – 436	Low – Medium
437 – 654	Medium
655 – 872	Medium – High
873 – 1090	High

Table 23: Overall inherent risk score range for Jurisdictions & Players

Jurisdiction & Players	Low risk	Low- Medium risk	Medium risk	Medium-High risk	High risk
Player jurisdictions	N/A				
PEPs	N/A				
High depositors	N/A				
High risk Players based on Payment methods	N/A				
TOTAL	SCORE: 0 = RISK: N/A				

Table 24: Overall inherent risk rating for Jurisdictions & Players

Initial


DS


2.4 Inherent risk – Delivery channels

Temple Holdings N.V. also assessed whether – and to what extent – the method of servicing the player could increase the inherent ML/FT risk.

As outlined in Curaçao's NRA and in the EU Supranational Risk Assessment: online gambling is exposed to a greater level of risk due to the huge volumes of transactions and the non-face-to-face nature of the business relationship.

The tables below contain the ranges of risk scores as well as the risk factor identified, and the inherent risk rating attributed in relation to the delivery channel.

Score Range Delivery Channel	Risk Rating
0 – 12	Low
13 – 25	Low – Medium
26 – 37	Medium
38 – 50	Medium – High
51 – 62	High

Table 25: Delivery channel – Inherent risk score range

Delivery Channel		
Risk factors	Answer	Score
Are players serviced on a non-face to face basis?	Yes (100% of our customer base)	62
Delivery Channel Risk	High	62

Table 26: Delivery channel – Inherent risk rating

2.5 Total inherent risk

The total inherent risk of the games, payment methods, jurisdictions & players, delivery channel and EU SNRA & Curaçao NRA have been aggregated to give a final inherent risk score, which is provided in the table below.

Overall Range Inherent Risk	Risk Rating
0 – 570	Low
571 – 1140	Low – Medium
1141 – 1710	Medium
1711 – 2280	Medium – High
2281 – 2852	High

Table 27: Overall inherent risk range

Category of risk	Low risk	Low-Medium risk	Medium risk	Medium-High risk	High risk
Games		324			
Payment methods				381	
Jurisdiction & Players			N/A		
Delivery channel					62
TOTAL	SCORE: 767 = RISK: Low-Medium				

Table 28: Overall inherent risk range

Please note: the above score is without analysing the Jurisdiction & Players Section.

3. Determination of risk appetite

Risk appetite can be defined as the level and type of risk that an entity is willing to take in order to meet strategic objectives.

The Board of Directors and Senior Management of the Company have established a strong AML/CFT culture within the organization and are consistently increasing their efforts on different fronts to ensure that AML/CFT remains a priority for the organization. The Company's ML/FT risk appetite is grounded in the over-arching principle that any transactions that may remotely or indirectly be linked or somehow connected to money laundering or funding of terrorism will not be tolerated, and that business with individuals or entities that might be engaged in such activities will not be entertained. Every effort is being made to minimize the possibility of products of the Company unwillingly being used by launderers or terrorist financiers.

The Directors of the Company have taken a commitment that Temple Holding N.V.'s overall risk appetite remains at least at a low-medium level by ensuring that adequate policies and procedures are implemented and applied in practice. Moreover, the Board together with the Senior Management has taken a number of decisions aimed at limiting risk, that are being listed below:

- Not allowing players to open more than one account per brand;
- Not accepting players (including temporary visitors) located in or residents of certain high-risk jurisdictions;
- Not offering high risk peer-to-peer gaming facilities;
- Obtaining information and, where necessary, documentation in relation to the source of funds / source of wealth of their customers;
- Only considering the acceptance of high-risk players once it is assured that appropriate controls have been applied to mitigate the risk;
- Not accepting any players posing a very high level of money laundering or terrorist financing risk;
- Dealing with reputable affiliates only;
- Dealing with reputable suppliers/3rd party providers only; and
- Carrying out effective transaction monitoring to ensure that any unusual activity is detected and investigated immediately.

Initial


DS


4. Analysis of AML/CFT controls

Following the identification and assessment of inherent risk, an evaluation was undertaken of the level and effectiveness of the AML/CFT controls that the Company has in place. The strength and effectiveness of the controls were assessed by an external Gaming Consultant company. It was examined whether existing controls are sufficiently robust to mitigate the Company's inherent risk and whether these are aligned with its risk appetite.

In view of the heightened risk identified within the sector in the EU Supranational Risk Assessment and the risk assessment carried out by the Curaçao National Risk Assessment, the expectations in respect of the controls implemented by online gambling companies to mitigate the non-face-to-face nature of the business are invariably expected to be higher. The assessment of the Company's controls has therefore taken this higher benchmark into account.

A breakdown of the strength of the controls per category is provided in the paragraphs hereunder.

4.1 Controls – Games

When assessing the controls in place in relation to games, all the games provided by the Company were assessed individually. The tables below provide the scoring range for controls in place for games, the control factors which impact specifically upon the games offered and the control rating per game type. Based on this assessment, the strength of the controls for each product category has been rated as shown below.

Although it resulted that the Company has controls in place that are effective in relation to games, there are certain areas which are either deficient or require improvements, as outlined in the below tables. The Company will be ensuring that these areas are improved.

Score Range Games	Control Rating
41 – 50	Satisfactory
31 – 40	Effective
21 – 30	Needs improvement
11 – 20	Poor
0 – 10	Deficient

Table 29: Games control score range

Casino games		
Control factors	Answer	Score
Are checks carried out by the game provider to identify irregular play, opposite betting- and suspicious activity?	Satisfactory	20
Does the game provider provide instant reporting on suspicious play?	Needs improvement	15
Has the monitoring done by the game provider been tested by Temple Holdings?	Deficient	0
Table games control	Effective	35

Table 30: Casino games – Control rating

Sports betting		
Control factors	Answer	Score
Are checks carried out by the game provider to identify irregular play, opposite betting- and suspicious activity?	Satisfactory	20
Does the game provider provide instant reporting on suspicious play?	Satisfactory	20
Has the monitoring done by the game provider been tested by Temple Holdings?	Deficient	0
Slots control	Satisfactory	40

Table 31: Sports betting – Control rating

Initial


DS


Virtuals		
Control factors	Answer	Score
Are checks carried out by the game provider to identify irregular play, opposite betting- and suspicious activity?	Satisfactory	20
Does the game provider provide instant reporting on suspicious play?	Satisfactory	20
Has the monitoring done by the game provider been tested by Temple Holdings?	Deficient	0
Live casino control	Satisfactory	40

Table 32: Virtuals – Control rating

The following tables provide the overall control scoring range for games and the overall control rating in relation to all games:

Overall Score Range Games	Control Rating
120 – 150	Satisfactory
90 – 119	Effective
60 – 89	Needs improvement
30 – 59	Poor
0 – 29	Deficient

Table 33: Overall control score range for Games

Games	Satisfactory	Effective	Needs improvement	Poor	Deficient
Casino games		35			
Sports betting	40				
Virtuals	40				
TOTAL	SCORE: 115 = CONTROL: Effective				

Table 34: Overall control rating for Games

4.2 Controls – Payment methods

Each payment method offered by Temple Holdings N.V. has been assessed in terms of controls with the help of the Senior Management. The following tables provide a control scoring range that varies for each of the payment methods due to the different control factors which impact specifically upon the payment methods offered and the control rating per payment type. Based on this assessment, the strength of the controls for each payment method has been rated as shown below.

The Company has identified that the controls in relation to payment methods require some improvement. There are certain areas which are deficient, such as the inability to have a closed looped policy on every payment method, the inability to identify players using multiple payment methods, the application of EDD measures and the technological tools in place to monitor and detect suspicious activity for AML purposes, as outlined in the tables below.

Score Range	Control Rating
Crypto Payments	
101 – 125	Satisfactory
76 – 100	Effective
51 – 75	Needs improvement
26 – 50	Poor
0 – 25	Deficient

Table 35: Crypto Payments control score range

Crypto Payments		
Control factors	Answer	Score
In cases where a closed loop policy is not possible, is the risk mitigated?	Needs improvement	10
Is there a limit on the number of crypto payments accepted per player?	Needs improvement	10
Is there a limit on the value uploaded?	Satisfactory	15
Is EDD carried out on players using crypto?	Needs improvement	5
Are players using multiple crypto wallets identified and monitored?	Needs improvement	5
How strong is the Anti-fraud and payments team?	Deficient	0
How effective are the technological tools in place to monitor and detect suspicious activity for AML purposes?	Deficient	0
Crypto payments control	Poor	45

Table 36: Crypto payments control rating

Initial
MC

DS
[Signature]

The following tables provide the overall control scoring range for payment methods and the overall control rating in relation to all payment methods:

Overall Score Range Payment methods	Control Rating
101 – 125	Satisfactory
76 – 100	Effective
51 – 75	Needs improvement
26 – 50	Poor
0 – 25	Deficient

Table 37: Overall Payment methods control score range

Payment methods	Satisfactory	Effective	Needs improvement	Poor	Deficient
Crypto payments				45	
TOTAL	SCORE: 45 = CONTROL: POOR				

Table 38: Overall Payment methods control score range

Initial


DS


4.3 Controls – Customer Due Diligence

The strength of the customer due diligence (CDD) carried out by the Company has also been assessed. Table 39 and 40 provide the control scoring range for CDD, the control factors which impact specifically on CDD, and the control rating for CDD. Based on this assessment, it was determined that controls in this area are:

Identification: the customer identification is being done when our customers registering a gaming account with us. We are asking for personal data set, such as first name, last name, date of birth, residential address, phone number, email address.

Verification: the customer verification is being done when our customers reached the mandatory KYC threshold EUR 2,000 – or equivalent in other currencies across brands. Customers can upload their KYC documents through an external, 3rd party provider who is supporting the verification of our players. If a document is out of date, we are receiving alerts to request up to date documentation from our players.

Information on source of funds/source of wealth: the Company has adopted a procedure whereby information in relation to the occupation, source of funds and source of wealth is obtained directly from the player when the risk is high. This information is then backed up with supporting documents to confirm either the source of funds, source of wealth or both on a later stage or when the AML risk is high.

Enhanced Due Diligence: EDD is currently being conducted on players who ought to be subjected to EDD, such as high-risk players, PEPs and where we have concerns about the funds used to deposit with us.

Multiple accounts: The Company is able to identify duplicate accounts.

PEP and Sanction screening: The Company adopted an external provider to carry out PEP and Sanctions screening. Sanctions screening happens on the first deposit attempt of the player, just as PEP check.

Ongoing Monitoring: To ensure that the documentation held on players are kept up-to-date and we have information and documentation related to source of funds and affordability. Also, the Company is monitoring customer transactions at different financial thresholds and upon withdrawal stages.

Initial


DS


Score Range	Control Rating
Customer Due Diligence	
245 – 306	Satisfactory
184 – 244	Effective
123 – 183	Needs improvement
62 – 122	Poor
0 – 61	Deficient

Table 39: CDD control score range

Customer Due Diligence Control		
Control factors	Answer	Score
Does the Company have adequate written policies and procedures for CDD/KYC principles?	Yes	3
Have these been reviewed and updated?	Yes	3
Have the policies and procedures been communicated to employees and management concerned?	Yes	6
Does the Company have an updated and documented Customer Acceptance Policy?	Yes	6
Is there a system for testing compliance with the CDD policies and procedures, and the AML/CFT legislation?	Deficient	0
Has the appropriate level of due diligence, including source of wealth and funds (where necessary), been applied on all players?	Needs improvement	25
Does the company collect information on the financial situation and occupation of all players who reach high risk?	Satisfactory	30
Have documents to support the source of wealth and source of	Needs improvement	25

funds of high depositors been collected (where necessary)?		
Have appropriate EDD measures been applied on all PEPs?	No	0
Have appropriate EDD measures been applied on all high-risk players?	Yes	30
Is due diligence applied on affiliates?	No	0
Are affiliate player accounts monitored for suspicious activity?	Yes	6
Have all customers been screened for PEPs and Sanctions?	No	0
Does the Company have a system in place to ensure that documents and information on players are kept up to date?	Yes	30
Are systems in place to assess changes in PEP and sanction status of the customers?	No	0
CDD control	Needs improvement	164
TOTAL	SCORE: 164 = CONTROL: Needs improvement	

Table 40: CDD control rating

Initial


DS


4.4 Controls – Delivery channels

The following tables provide the control scoring range in relation to the delivery channel, the control factors which impact specifically upon the delivery channel used, the control rating for the channel used. Based on this assessment, it was identified that the delivery channel is satisfactory in its controls since the Company has implemented a face verification tool (3rd party provider) in order to mitigate the non-face-to face risk of the Company.

Score Range Delivery channel	Control Rating
49 – 60	Satisfactory
37 – 48	Effective
25 – 36	Needs improvement
13 – 24	Poor
0 – 12	Deficient

Table 41: Delivery channel control score range

Delivery channel		
Control factors	Answer	Score
Are technological measures in place to mitigate the non-face to face risk?	Yes	30
Where a technological measure is not in place, is EDD being applied?	Yes	30
Delivery channel control	Satisfactory	60

Table 42: Delivery channel control rating

4.5 Controls – Risk assessment

The tables hereunder illustrate the control scoring range adopted in relation to the risk assessment carried out by the Company, the control factors which impact specifically upon the risk assessment conducted, the control rating for the assessment carried out, as well as the Curaçao FIU audit results. Based on this assessment, the strength of the controls for risk assessment has been rated as Deficient. Temple Holdings N.V. need to introduce a new in-house tool, which will risk rate customers. The risk rating is determined based on a number of fields and scores assigned to particular factors. When a player's risk rating changes, an alert should be generated which will necessitate a review of the player account.

Score Range Risk Assessment	Control Rating
164 – 205	Satisfactory
123 – 163	Effective
83 – 122	Needs improvement
42 – 82	Poor
0 – 41	Deficient

Table 43: Risk Assessment control score range

Risk Assessment		
Control factors	Answer	Score
Does the Company have an ML/FT risk classification system in place that differentiates between lower and higher risk customers?	Deficient	0
How adequate is the risk assessment criteria that is being used?	Deficient	0
Have all the Company's players been adequately risk assessed?	No	0
Is an automated risk assessment tool used?	No	0
Are there processes to review client's risk profile?	No	0
How effective are the triggers in place to alert the Company that a player may have suddenly become higher risk?	Deficient	0
Are the Board and senior management kept abreast of changing ML/FT risk? If so, how is this communicated?	Yes	25
Risk assessment control	Deficient	25

Table 44: Risk Assessment control rating

Initial
MC

DS
[Signature]

4.6 Controls – Transaction monitoring and reporting

The tables hereunder provide the control scoring range applicable in relation to transaction monitoring and reporting carried out by Temple Holdings, the control factors which impact specifically upon the monitoring and reporting conducted, the control rating in place for the monitoring and reporting carried out. Based on this assessment, the strength of the controls for transaction monitoring and reporting has been rated as Needs improvement.

Score Range	Control Rating
Transaction monitoring	
129 – 162	Satisfactory
97 – 128	Effective
65 – 96	Needs improvement
33 – 64	Poor
0 – 32	Deficient

Table 45: Transaction monitoring and reporting control score range

Transaction monitoring and reporting		
Control factors	Answer	Score
Does the Company have an adequate policy on transaction monitoring and reporting for AML purposes?	Yes	5
Does the company have an effective system to detect unusual transactions for AML purposes?	Needs improvement	25
Does the company have enough employees to monitor transactions effectively for AML purposes?	Deficient	0
Is the company's reporting procedure adequate?	No	0
Are all employees aware of suspicious behaviour and what should be done when knowledge or suspicion of ML/FT is present?	Needs improvement	25
Has the company informed staff of the procedures for internal reporting of unusual/suspicious activity/transactions ('internal reports') to the MLRO?	Yes	11
How many internal unusual transaction reports were raised from January 2024 until present?	None	0
How many of these UTRs have resulted in a disclosure to the FIU?	None	0
What is the average time it takes the MLRO to review such reports and make a prima facie determination?	Cannot determine...	0
Transaction monitoring and reporting control	Needs improvement	66

Table 46: Transaction monitoring and reporting control rating

Initial
MC

DS
[Signature]

4.7 Controls – Internal audit

The following tables provide the scoring range in relation to the internal audit function of Temple Holdings, the control factors which impact specifically upon the internal audit function, the control rating for this function. Based on this assessment, the strength of the controls for internal audit has been rated as Deficient. The Company at a later stage can either develop an internal audit function or ask an external company who can review and test the AML/CFT program together.

Score Range Internal Audit	Control Rating
40 – 48	Satisfactory
30 – 39	Effective
20 – 29	Needs improvement
10 – 19	Poor
0 – 9	Deficient

Table 47: Internal audit control score range

Internal Audit		
Control factors	Answer	Score
Does the Company have an Internal or external Audit Department/function?	No	0
Has the AML/CFT program been reviewed and tested?	No	0
Internal Audit control	Deficient	0

Table 48: Internal audit control rating

Initial
MC

DS
[Signature]

4.8 Controls – Record keeping

The following tables provide the scoring range in relation to record keeping, the control factors which impact specifically upon record keeping and the control rating. Based on this assessment, the strength of the controls for record keeping has been rated as effective. Need to be noted, that the Company should later on hire a Data Protection Officer (DPO), who will be responsible to test the record keeping procedures.

Score Range Record keeping	Control Rating
46 – 56	Satisfactory
35 – 45	Effective
23 – 34	Needs improvement
12 – 22	Poor
0 – 11	Deficient

Table 49: Record keeping control score range

Record Keeping		
Control factors	Answer	Score
Has this record keeping procedure been tested?	Yes	5
Do records provide a clear audit trail?	Needs improvement	19
How long would it take to retrieve the information for a particular customer going back 5 years?	Between 2 and 5 days	12
Has there ever been a request for information from the authorities (e.g. Curaçao FIU) for customer data where information could not be provided?	N/A	0
Has the casino asked for an extension from the authorities in order to be able to meet these requests for information?	No	5
Record Keeping control	Effective	41

Table 50: Record keeping control rating

4.9 Controls – Training and HR

The following tables provide the scoring range applied in relation to training of employees of Temple Holdings in relation to AML/CFT and to the vetting of employees, the control factors which impact specifically these areas, the control rating, as well as any audit results. Based on this assessment, the strength of the controls for training and HR has been rated as Deficient.

Training: The nominated Compliance Officer/MLRO should provide an AML/CFT training to the employees of Temple Holdings, also providing specific training in relation to their AML/CFT obligations. This training should include the Board of directors and Senior management of the Company.

Vetting of Employees: The Company is requesting documentation prior to recruiting a new employee and carry out screening to identify whether the employee has a criminal record.

Score Range Training and HR	Control Rating
63 – 78	Satisfactory
48 – 62	Effective
32 – 47	Needs improvement
17 – 31	Poor
0 – 16	Deficient

Table 51: Training and HR control score range

Training and HR		
Control factors	Answer	Score
Is the company's staff trained to understand how AML/CFT applies to their specific model and the roles they undertake?	Deficient	0
What is the frequency of AML/CFT training provided?	Yearly	4
Does the Company provide internal AML/CFT training to employees?	No	0
Has the Board and senior management participated in AML/CFT training?	No	0
Are staff tested for knowledge retention following AML/CFT training?	No	0
Does the company screen prospective employees (e.g. criminal records)?	Yes	5
Is staff screened for criminal record during employment?	No	0
Training and HR control	Deficient	9

Table 52: Training and HR control rating

Initial
MC

DS
[Signature]

4.10 Controls – MLRO and compliance

The control scoring range in relation to the function of the MLRO and the Compliance Department is provided in the tables below, together with the control factors which impact specifically these areas, the control rating. Based on this assessment, the strength of the controls for the MLRO and Compliance function has been rated as shown below.

The strength of the control was rated as Deficient, and it should be noted that the Company should set up a compliance/legal department.

Score Range MLRO and compliance	Control Rating
134 – 166	Satisfactory
101 – 133	Effective
67 – 100	Needs improvement
34 – 66	Poor
0 – 33	Deficient

Table 53: MLRO and compliance control score range

MLRO and compliance		
Control factors	Answer	Score
Has the Company appointed an MLRO?	No	0
How effective is the MLRO in carrying out his duties?	Deficient	0
Does the MLRO carry out other duties besides AML/CFT?	N/A	0
What proportion of time is devoted to AML/CFT issues?	N/A	0
Is the MLRO able to act independently?	N/A	0
Is the MLRO able to communicate easily and effectively with the Board?	N/A	0
Does the MLRO receive support from senior management?	N/A	0
Does the MLRO have access to all records, data and documentation?	N/A	0
Is there a compliance unit?	No	0
How many employees make up this unit?	None	0
How much of the Fraud unit's time is dedicated to AML/CFT?	Less than 50	0
How many employees make up this unit?	Less than 3	6
Do the employees have some experience working in AML/CFT compliance?	Needs improvement	6
MLRO and compliance control	Deficient	12

Table 54: MLRO and compliance control rating

Initial
MC

DS
[Signature]

4.11 Controls – Governance

The scoring range in relation to the Governance function, the control factors which impact specifically this area, and the control rating are included in the tables below. Based on this assessment, the strength of the controls for the Governance function has been rated as Needs improvement.

It should be highlighted that the Company have an adequate AML/CFT procedures manual in place and the Board receive or discuss compliance issues as needed.

Score Range Governance	Control Rating
90 – 111	Satisfactory
68 – 89	Effective
45 – 67	Needs improvement
23 – 44	Poor
0 – 22	Deficient

Table 55: Governance control score range

Governance		
Control factors	Answer	Score
Does the Company have written AML/CFT procedures?	Satisfactory	5
Has the Board designated any of its members responsible for AML/CFT issues?	Needs improvement	6
Does the Board/ Senior management ensure that the AML/CFT program, including risk management, is effectively implemented by all relevant departments?	Needs improvement	25
Does the Board receive reports or updates on AML/CFT issues and programs?	Needs improvement	25
Are AML/CFT related matters discussed at least once quarterly?	Needs improvement	2
Is the MLRO of sufficient seniority to influence the board?	N/A	0
Governance control	Needs improvement	63

Table 56: Governance control rating

4.12 Controls – Outsourcing

All outsourcing relationships hold risks. Being aware of the potential risks involved and having ability to monitor, evaluate and manage these risks is crucial for the Company.

The scoring range in relation to the Outsourcing function, the control factors which impact specifically this area, and the control rating are included in the tables below. Based on this assessment, the strength of the controls for the Outsourcing function has been rated as Satisfactory.

It should be highlighted that the Company have an adequate AML/CFT procedures manual in place to control the risk derived from outsourcing such functions as our AML/CFT obligations.

Score Range Outsourcing	Control Rating
121 – 150	Satisfactory
91 – 120	Effective
61 – 90	Needs improvement
31 – 60	Poor
0 – 30	Deficient

Table 57: Outsourcing control score range

Outsourcing		
Control factors	Answer	Score
Does the outsourcing negatively prejudice the Company's ability to comply with its obligations at law and the effectiveness of the Company's compliance and audit functions?	Satisfactory	30
Does the third party have the necessary resources, qualifications, skills and authorisations (if required) at its disposal to effectively carry out the measures and procedures to perform on behalf of the Company?	Needs improvement	25
Does the manner in which the third party proposes to implement the General Outsourced Activities on behalf of the Company is in line with all applicable legal requirements and the Company's own policies and procedures?	Needs improvement	25
Is the third party in good standing? (There being no adverse information in its regard, and it is located and operating from Curaçao, an EU Member State or another reputable jurisdiction)	Yes	30
Is the third party not subject to any obligation that would lead to a breach of any data protection, professional secrecy, confidentiality or non-disclosure obligation to which the Company has to adhere?	Yes	30
Outsourcing control	Satisfactory	140

Table 58: Outsourcing control rating

4.13 Overall controls

The control scored for each of the above factors assessed have been aggregated to give a final overall control score which is provided in the table below.

Overall Score Range Controls	Control Rating
1293 – 1617	Satisfactory
970 – 1292	Effective
647 – 969	Needs improvement
324 – 646	Poor
0 – 323	Deficient

Table 59: Overall controls score range

Category of controls	Satisfactory	Effective	Needs improvement	Poor	Deficient
Games		115			
Payment methods				45	
Customer Due Dil.			164		
Delivery channels	60				
Risk Assessment					25
Transaction monitoring			66		
Internal audit					0
Record keeping		41			
Training and HR					9
MLRO and compliance					12
Governance			63		
Outsourcing	140				
TOTAL	SCORE: 742 = CONTROL: Needs improvement				

Table 60: Overall rating for controls

As we can see in the table above (Table 60) some of the controls are satisfactory in mitigating some of the risks of money laundering and terrorist financing to which the Company is exposed, however some of these controls needs improvement.

5. Determination of residual risk

The assessment concluded that the Company’s total inherent risk is set at **medium**. This rating is derived from the assessment of the nature of the games offered, the type of payment methods the Company accepts, the type and volume of players it entertains, and the delivery channels it uses to onboard players. The strength of the Company’s AML/CFT controls to mitigate such risks were also assessed and rated as **Needs improvement**.

The residual risk is made up of the Company’s inherent risk and the controls the Company has in place to mitigate those risks. The residual risk of the Company is presented using the heatmap in Table 76 below which is a standard template used for ML/FT risk assessments. Temple Holdings N.V.’s overall residual risk has been determined to be **Low-medium**.

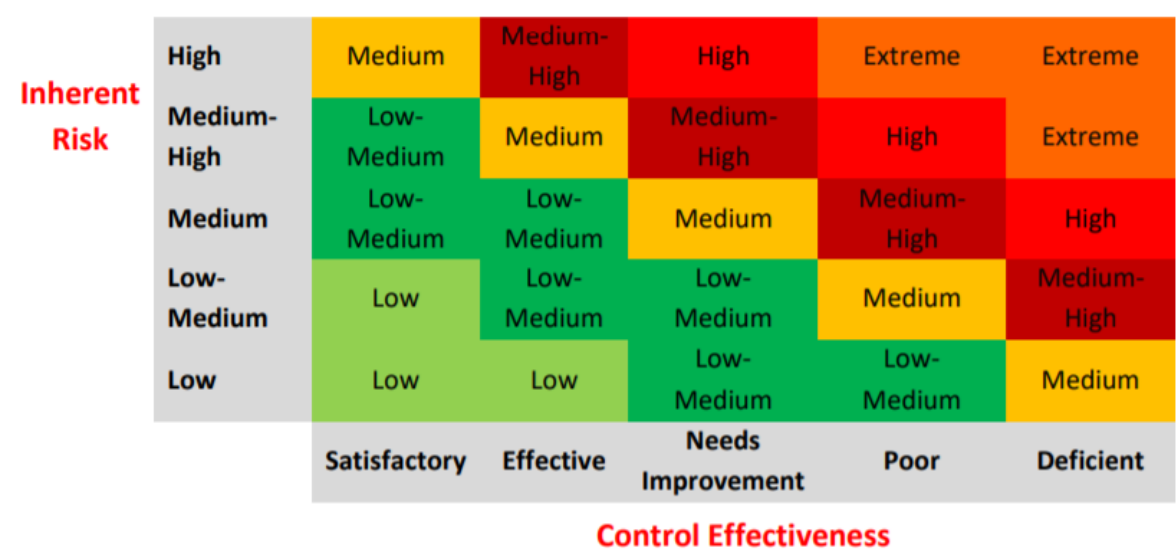


Table 61: Residual risk heatmap

The residual risk applicable in relation to games, payment methods, jurisdictions and players, delivery channels and risk assessment is broken down in the sections hereunder.

5.1 Residual risk – Games

The score for the overall residual risk of games is presented in the table below, taking into consideration the results of the inherent risk and the strength of controls calculated previously in relation to each type of game.

Games	Inherent Risk	Control Strength	Residual Risk
Casino Games	Low – Medium	Effective	Low – Medium
Sports Betting	Medium	Satisfactory	Low – Medium
Virtuals	Low – Medium	Satisfactory	Low
Overall Residual Risk - Games	Low – Medium	Satisfactory	Low

Table 62: Overall residual risk rating - Games

5.2 Residual risk – Payment methods

Payment methods	Inherent Risk	Control Strength	Residual Risk
Crypto Payments	Medium – High	Poor	High
Overall Residual Risk – Payment methods	Medium - High	Poor	High

Table 63: Overall residual risk rating - Payment methods

5.3 Residual risk – Jurisdictions and players

When calculating the residual risk arising from the jurisdiction risk and customer base, the controls in place that relate to customer due diligence, risk management, transaction monitoring and reporting, internal audit, record keeping, training and HR, the strength of the function of the MLRO and the Compliance Department as well as governance were considered. For the inherent risk, the category was grouped under the single heading of ‘Jurisdictions and Players’.

Players	Inherent Risk	Control Strength	Residual Risk
Player jurisdictions	N/A	N/A	N/A
PEPs	N/A	N/A	N/A
High depositors	N/A	N/A	N/A
High risk players	N/A	N/A	N/A
Overall Residual Risk – Players	N/A	N/A	N/A

Table 64: Overall residual risk rating - Players

5.4 Residual risk – Delivery channels

The scoring for the overall residual risk of delivery channels being used took into consideration the results of the inherent risk and the strength of controls calculated previously in relation to the delivery channel.

Delivery channel	Inherent Risk	Control Strength	Residual Risk
Overall Residual Risk – Delivery channel	High	Satisfactory	Medium

Table 65: Overall residual risk rating - Delivery channel

5.5 Total residual risk

The total residual risk of the games, payment methods, jurisdictions & players, delivery channel have been aggregated to give a final residual risk score which is provided in the table below.

Category of risk	Low risk	Low-Medium risk	Medium risk	Medium-High risk	High risk
Games	X				
Payment methods		X			
Jurisdiction & Players			N/A		
Delivery channel			X		
TOTAL	RISK: Low – Medium				

Table 66: Overall residual risk range

Summary of Overall residual risk for:

- Games: **Low**
- Payment methods: **Low - Medium**
- Players & Jurisdictions: N/A
- Delivery channel: **Medium**

Residual risk is the level of risk left after applying the mitigating measures, policies, controls and procedures to the level of inherent risk identified. Level of inherent Risk - Mitigating Measures = Level of Residual Risk. Overall residual risk of the business is **Low-Medium**

6. Remediation plan

Temple Holdings N.V. is committed to keep working to improve its controls to ensure that the residual risk of the Company is reduced and to also ensure, on a consistent basis, that any gaps identified are remediated as a matter of priority.

A list of action points has been drawn up, outlined in the table below, that the Company will be actioning depending on the priority set to each action point:

HIGH PRIORITY	
Nominate a Compliance Officer / MLRO	It is GCA's requirement that the Company must nominate a Compliance Officer / MLRO. „ <i>The casino shall formally designate a senior officer at management level and independent from the games operations, responsible for the detection and deterrence of money laundering and terrorist financing. The AML/CFT compliance officer must have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The compliance officer must be able to act independently.</i> ”
The Company should design a Customer Risk Assessment	“<i>The customer specific risk assessment has to be carried out either prior to the carrying out of an occasional transaction, or during establishing a business relationship. It is possible that this initial customer specific risk assessment will have to be revised at a later stage of the business relationship and this may result in a customer's risk rating having to be adjusted.</i> <i>The Customer Risk Assessment will assess the particular risks the casino will be exposed to when providing its services or products to players. The information collected to draw up the CRA will formulate the customer's risk profile.</i>”
PEP & Sanctions screening	It is imperative that the customers of the Company are screened against Sanctions lists defined by GCA and also going through PEP checks. The Company is working together with a 3 rd party provider who provides this service, however the Company must ensure these checks will be carried out upon first deposit (or first deposit attempt).

MEDIUM PRIORITY	
Internal audit function	When the Company is up and running later on it would be beneficial to have an internal audit function or to run an external audit to have a gap analysis on the Company's various departments.
Introducing other (low risk) payment methods	At this stage the Company has only one payment method (crypto via Coinspaid) which is medium-high risk from an AML perspective. It would be a risk mitigating factor if the Company can introduce different payment methods, which are lower risk for the Company.
Transaction monitoring system	The Company must monitor all transactions when it will launch its brand. This is crucial in order to avoid that the Company is used for money laundering / terrorist financing purposes by its customers.

LOW PRIORITY	
Formulate a separate KYC, Fraud & AML Department	Based on the Company's volumes at a later stage it is highly recommended to formulate a separate department who can carry out KYC, Fraud and AML related tasks. Or there is a possibility also to outsource such function.
Employee screening and training	With the growth of the Company, it should also carry out PEP & sanctions screening on their future employees and provide them training depends on their functions.

7. Conclusion

This document describes the purpose, scope and methodology used for the business risk assessment of Temple Holdings N.V. and provides an overview of its conclusions.

Through the assessment it was concluded that presently the Company faces an overall residual risk of Low-medium which poses a considerable risk in terms of AML/CFT. In this regard there are a number of actions that are considered necessary for Temple Holdings to take to ensure that the Company's processes are brought in line with all its obligations and to safeguard it from being used as a vehicle for ML/FT.

A number of recommendations are therefore being made in this report.

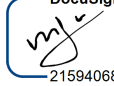
Appendix I – Business Risk Assessment excel sheet (scoring and weighing)

The Appendix can be found on a separate excel sheet, which will be always provided together with this Business Risk Assessment.

Initial


DS


Board of Directors signature page

DocuSigned by:

215940689FEB429...

16/05/2025

Starkeast Management B.V., Managing Director

By: Menno Jordaan, as director of Starkeast Management B.V.

Signed by:

C844330A35F54B6...

16/05/2025

Mark Cauchi

Key Compliance / MLRO

Initial


DS
