



Digitain Curacao B.V.

Digitain Curacao B.V. Policy and Procedure for Combating Money Laundering, the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction

Date: March, 2025

Contents

1. Glossary	2
2. Overview and Commitment to Compliance.....	2
3. Overview of Money Laundering (ML)	3
4. Overview of Financing of Terrorism (FT)	3
5. Overview of Financing of Proliferation of weapons (FP)	4
6. Compliance with Targeted Financial Sanctions	4
7. Risk-Based Approach	4
8. Client/Partner Onboarding, Due Diligence and Compliance Assurance	6
9. Customer Acceptance Policy.....	7
10. Business Partner/Client Onboarding and Due Diligence Process.....	7
11. Identification of Risk.....	8
12. Training and Awareness.....	9
13. Record Keeping and Documentation.....	9
14. Audit and Internal Controls.....	10
15. Digitain Statement.....	10

1. Glossary

Terms/Abbreviations	Description
Gambling	Gambling is the act of risking something of value, typically money, on an event or game whose outcome is largely determined by chance, with the aim of winning a prize or reward. It generally involves three key elements: consideration (the stake or wager), risk (the uncertainty or chance involved) and a potential prize (the reward or gain if successful).
CGA	Curacao Gaming Authority
CFATF	The Caribbean Financial Action Taskforce. an organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.

FATF	The Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
FATF Recommendations	A framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;
FIU	The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.
Supplier License	Means a license for offering Critical Services or Goods;
Client/Partner	Any individual, company, or entity that enters into a business relationship with DIGITAIN CURACAO B.V. for the provision of iGaming services, including B2B, B2C partners, third-party service providers.
B2B	Business to Business. It describes transactions or interactions that occur between two businesses, as opposed to between a business and individual consumer (which is referred to as B2C, or Business-to-Consumer). In a B2B model, one company sells products or services to another company.
B2C	Business to Consumer. It describes the transactions or interactions between a business and individual customer, where the business directly sells goods or services to the end user.

2. Overview and Commitment to Compliance

DIGITAIN CURACAO B.V. (hereinafter referred to as “Digitain” or “the Company”) a company incorporated in Curacao, is registered with the Chamber of Commerce under registration number [162596] and holds a valid gaming license under license number [OGL/2024/887/0618]. As a fully licensed entity, we specialize in providing software services to business partners within the iGaming industry, operating under the regulations set by the Curacao Gaming Control Board (GCB). Our operations are conducted in strict adherence to all applicable local regulations, including those governing anti-money laundering (AML), counter-financing of terrorism (CFT) and the prevention of the proliferation of weapons of mass destruction. We are committed to maintaining the highest standards of integrity and compliance in all our business activities.

This procedure is designed to protect DIGITAIN from being misused for illegal activities, including money laundering, terrorist financing and weapons proliferation of mass destruction. Our commitment to

compliance ensures that we uphold our good standing with regulatory bodies, foster trust with our business partners and prevent any misuse of our services for illicit purposes.

Digitain recognizes the critical importance of safeguarding its services against potential criminal misuse. We are fully dedicated to complying with both local and international laws, regulations and industry standards governing the iGaming sector in Curaçao as well as AML/CFT/FP obligations.

In accordance with the regulations set forth by the Curaçao Gaming Control Board (GCB), Digitain implements and enforces robust policies and procedures to detect, prevent and report any suspicious activities related to ML, FT or FP.

Digitain is committed to ensuring the highest standards of integrity, transparency and accountability. We are resolute in maintaining full compliance with both local and international obligations and our procedure will undergo regular reviews to ensure its continued relevance and effectiveness in addressing evolving risks in a dynamic regulatory environment.

This procedure applies to all operations undertaken by Digitain within the iGaming sector, including but not limited to B2B services related to fast games and online casinos. It extends to all departments, employees, partners and third-party service providers involved in or supporting these activities, ensuring comprehensive adherence across all levels of the organization. By doing so, we maintain strict compliance and uphold the integrity of our business operations.

3. Overview of Money Laundering (ML)

Money laundering (ML) is the process by which criminals conceal the true origin and ownership of illegally obtained funds, making them appear legitimate. This process typically occurs in three distinct phases. **Placement** is the initial stage, where illicit funds are introduced into the financial system through various means, such as purchasing casino chips with cash, funding gaming accounts, or utilizing credit/debit cards, prepaid cards, checks, or cryptocurrencies. At this stage, the funds may be immediately withdrawn or redeemed for credits, often without engaging in actual gambling activities. The second phase, **Layering**, involves moving or converting the funds to obscure their origin and ownership. This is done through multiple transactions, such as transferring funds between accounts, using casinos or financial institutions to move money across jurisdictions, engaging in currency exchanges and employing complex gambling strategies. The goal of layering is to create a series of transactions that make it difficult for authorities to trace the source of the funds. The final phase, **Integration**, sees the laundered money being reintroduced into the economy in a way that appears legitimate. This can involve purchasing luxury goods, making investments, or entering into business dealings, thereby blending the illegal funds with lawful ones. Each stage of the process is designed to obscure the illegal nature of the funds, making it more difficult for authorities to detect and prevent money laundering activities.

4. Overview of Financing of Terrorism (FT)

Financing of Terrorism (FT) refers to the process of providing funds to support terrorist activities, individuals, or organizations. Unlike money laundering (ML), the funds used for terrorism financing may not always be sourced from illicit activities. Instead, they are typically used to further political, social, or religious motives. Terrorism financing can involve a wide array of methods designed to conceal the origin and destination of the funds. Common techniques include cash smuggling, wire transfers, structuring payments to avoid detection, purchasing monetary instruments such as traveler's checks or money orders and using debit or credit cards to obscure the recipients of the funds. The ultimate goal of terrorism financing is to enable or facilitate terrorist activities, regardless of the legitimate or illicit origins of the funds.

5. Overview of Financing of Proliferation of weapons (FP)

Financing of Proliferation refers to the provision of funds to support the development, acquisition, transportation, or stockpiling of weapons of mass destruction (WMDs), including nuclear, chemical and biological weapons. Entities involved in the proliferation of such weapons often utilize techniques akin to money laundering to obscure the origin and destination of these funds. These methods may involve complex financial transactions, front companies and other mechanisms designed to bypass regulatory scrutiny and conceal the true purpose of the financial activities. The goal of proliferation financing is to support the spread of weapons that pose significant threats to international security and stability.

6. Compliance with Targeted Financial Sanctions

Targeted financial sanctions require countries to freeze funds and assets and ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities. As part of its commitment to maintaining the highest standards of compliance, **DIGITAIN**, actively engaged in the iGaming sector and providing B2B services to key partner companies in fast games and online casino gaming, acknowledges its responsibility to adhere to these sanctions requirements.

All natural and legal persons in Curaçao, including **DIGITAIN**, are required to freeze without delay and without prior notice the funds or other assets of designated persons and entities. This is in compliance with United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations and EU sanctions are binding for Curaçao under the Kingdom Sanctions Act.

In cases where sanctioned individuals or organizations are identified, a report is promptly filed with the Financial Intelligence Unit (FIU) and the company follows the prescribed process for the freezing of resources.

Additionally, **DIGITAIN** recognizes the importance of staying up-to-date with any amendments to Sanctions Decrees and Regulations. As such, the company conducts regular checks for updates and promptly revises its Customer Due Diligence (CDD) and Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) policies and procedures to reflect these changes.

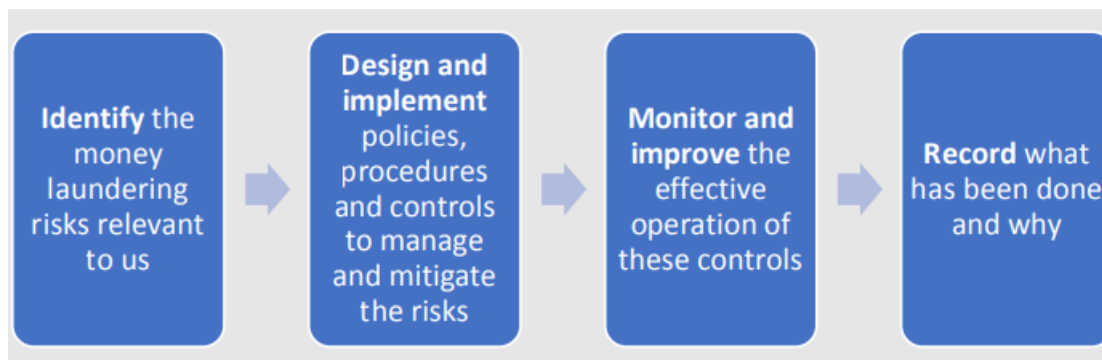
By enforcing these rigorous standards, DIGITAIN remains dedicated to mitigating the risk of financial crime and upholding the integrity of the online gaming industry.

7. Risk-Based Approach

In line with international Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) standards, Digitain adopts a Risk-Based Approach to ensure that its AML/CFT measures are tailored to address the specific risks identified in its operations. This approach involves conducting regular and comprehensive risk assessments to evaluate the potential risks associated with money laundering, terrorist financing and the financing of proliferation of weapons activities. The assessment takes into consideration key factors, including the geographical location of Clients, the nature of the products and services offered and the customer profiles.

Based on the findings of the risk assessment, Digitain implements appropriate mitigation measures. Higher-risk areas will be subject to Enhanced Due Diligence (EDD), ensuring more stringent oversight. Ongoing monitoring processes are in place to evaluate the effectiveness of these controls, enabling the identification and mitigation of emerging risks. This ensures that the company's AML/CFT measures remain relevant and effective in addressing evolving threats.

A risk-based approach entails a series of strategic steps designed to implement the most proportionate and effective methods for managing and mitigating the risks faced by Digitain. The Company will adopt the following approach to ensure that its risk management processes are both comprehensive and aligned with best practices:



As part of its commitment to Anti-Money Laundering (AML), Counter-Financing of Terrorism (CFT) and Proliferation Financing (CPF) compliance, Digitain ensures that a robust risk assessment is performed to identify and mitigate potential risks associated with money laundering, terrorist financing and proliferation financing. This risk assessment is reviewed regularly and whenever significant changes occur, including the introduction of new products, business practices, technologies, or changes in Client demographics.

Such risk assessment must be appropriate and must be reviewed as necessary in the light of any changes of circumstances, including the introduction of new products, business practices or technology, new methods of payment by Clients. As part of such risk assessment, we will consider the factors listed below

- a) our Clients;
- b) the countries or geographic areas in which we operate;
- c) our products or services;
- d) transactions we are involved in; and
- e) our delivery channels.

Following completion of and having regard to the risk assessment and any review of the assessment, we must ensure we have appropriate policies, procedures and controls to prevent money laundering, terrorist financing and proliferation financing. We must ensure that our AML, CTF and CPF policies, procedures and controls are implemented effectively, kept under review, revised appropriately to ensure that they remain effective.

Digitain recognizes the potential risks, including the use of platforms for money laundering, terrorism financing, fraud and other illicit activities. In this regard, Digitain is committed to the strict adherence of all applicable Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) laws and regulations. The company pledges to implement the following measures:

1. Promoting a Robust Financial Crime Prevention Culture

Establishing and fostering a corporate culture dedicated to preventing financial crime and the financing of terrorism.

2. Thorough Onboarding and Continuous Monitoring of B2B Partners

Ensuring that all partners/clients are onboarded through a comprehensive due diligence process, including thorough verification in accordance with the company's "Know Your Client" (KYC) protocols. Ongoing monitoring will be conducted to maintain the same level of scrutiny throughout the duration of the business relationship.

3. Ensuring Compliance with AML/CFT Standards

Requiring that all business partners adopt and implement stringent measures and procedures aimed at preventing financial crime, terrorism financing and fraud, in full compliance with regulatory and licensing requirements.

4. Staff Training and Legal Awareness

Providing regular and thorough training for all staff to ensure they are fully aware of Digitain's obligations under the relevant legal and regulatory frameworks. This includes the proper reporting channels for any suspicious, illegal, or fraudulent activity.

By upholding these principles, Digitain ensures its continued commitment to combatting financial crime and ensuring the integrity of the online gaming environment.

8. Client/Partner Onboarding, Due Diligence and Compliance Assurance

Digitain recognizes the inherent risks associated with its B2B and B2C business partners/clients, which may be vulnerable to misuse for illegal activities such as money laundering (ML), terrorism financing (TF), fraud and other criminal offenses. As part of our unwavering commitment to mitigating these risks, Digitain adheres strictly to all applicable Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) regulations. Our approach ensures the highest standards of integrity, transparency and compliance across all operational levels, including:

Digitain is dedicated to fostering a corporate culture that prioritizes the prevention of financial crime, including money laundering and the financing of terrorism. This culture is integral to both internal operations and extends to all relationships with B2B/B2C partners and third-party vendors. We continuously emphasize compliance across all organizational levels, ensuring active deterrence and prevention of financial crime and terrorism financing.

- Digitain ensures that all potential B2B and B2C partners are onboarded through a comprehensive and robust due diligence process, fully compliant with our "Know Your Client" (KYC) requirements. The process includes:
 - We conduct extensive background checks to assess potential connections to money laundering, terrorism financing, or other illicit activities, based on risk factors including the partner's geographical location and business operations.
 - Compant implements continuous monitoring procedures to ensure that all business partners maintain regulatory compliance throughout the course of their partnership. This includes regular checks to ensure that partners' operations align with our compliance standards.
- Digitain requires its B2B and B2C partners to adopt and implement robust measures and procedures to prevent financial crime, including terrorism financing and fraud. These measures must align with the following:
 - **AML/CFT Compliance:** Partners must comply with applicable AML and CFT regulations, licensing requirements and international best practices.
 - **KYC Procedures:** Partners are required to implement stringent KYC procedures to verify and authenticate the identities of their end users, which is crucial in preventing illegal activities such as money laundering and fraud.
 - **Fraud Prevention Measures:** B2B and B2C partners must establish effective fraud detection systems to mitigate the risk of fraudulent activities, including transaction monitoring and suspicious activity reporting.

- Digitain ensures that all employees, are adequately trained on their AML/CFT obligations. This training includes:
 - Employees will receive training on relevant legal and regulatory obligations, including detecting and reporting suspicious, illegal, or fraudulent activities. This training is conducted regularly to ensure staff remain up to date with emerging risks and evolving compliance requirements.
 - Employees will be informed about the appropriate channels for reporting unusual or illegal activity. These channels ensure that suspicious activities are promptly reported to the relevant authorities in compliance with legal obligations.
 - To ensure continuous compliance, staff will receive periodic updates and reminders regarding new regulatory developments, evolving threats and best practices for preventing financial crime.

An essential component of the onboarding process for any business partner that the Company intends to engage with is a comprehensive risk-based due diligence assessment. This process evaluates various risk factors, including the partner's background, geographic location and the nature of the services or products they provide. Based on these factors, each partner is assigned a risk rating (Low, Medium, or High), which determines the scope and depth of the due diligence to be conducted. Every business partner is subject to a rigorous due diligence and screening procedure to ensure compliance and mitigate potential risks.

9. Customer Acceptance Policy

An integral part of the onboarding of any business partner Digitain wishes to get involved with, concerns a risk based due diligence. The risk factors related to the background of the party, their geographic position and the services or products that are provided to them are carefully assessed and a risk qualification is given to them (Low - Medium – High) on the basis of which the due diligence will be carried out.

10. Business Partner/Client Onboarding and Due Diligence Process

All business partners undergoing the onboarding process with Digitain will be subject to thorough screening, including checks for Sanctions, Relevant Adverse Information (RAI) and any potential involvement with or exposure to Politically Exposed Persons (PEPs). In addition, based on the partner's risk classification, a specific set of documents and/or information will be required for identification and verification purposes.

Any business partner failing to meet the standards set by Digitain or who receives negative screening results that cannot be effectively disputed, will not be further engaged by the company. In the event of negative screening results arising from an existing business relationship, the Company will take appropriate action, which may include suspending the relationship while a comprehensive Enhanced Due Diligence process is completed. If necessary, the relationship may be terminated, or conditions will be determined under which it may continue.

The following key areas are, at a minimum, included in the due diligence checks conducted by Digitain:

- Casino Operator Information
- An overview of the URLs associated and its target markets
- A summary of the partner/client shareholders and representatives
- A review of the licenses held by the partner/client

11. Identification of Risk

Digitain's policies, procedures and controls align with the Financial Action Task Force (FATF) recommendations to adopt a risk-based approach. This approach enables Digitain to identify its primary sources of risk, assess their nature and magnitude and allocate resources effectively to manage the most significant risks.

Digitain is committed to identifying and mitigating risks for several key reasons, including:

- Ensuring compliance with regulatory and licensing obligations.
- Preventing license suspension, revocation, imposition of fines and potential criminal prosecution.
- Protecting its reputation and avoiding adverse media attention.

Digitain has carefully evaluated the risks associated with its business operations, identifying the following primary areas of exposure:

To verify the identity and integrity of its business partners, their officers, employees and ultimate beneficial owners (UBOs), Digitain relies on Know Your Customer (KYC) procedures and continuous monitoring mechanisms. Additionally, the Company employs a variety of trusted sources to assess the identity and reputation of its B2B partners, including questionnaires completed by the partners, certified official documentation (translated where necessary) and open-source information from verified official sources such as government and regulatory websites, as well as government watch lists. Furthermore, Digitain conducts thorough PEP (Politically Exposed Persons) and sanction screenings, as well as adverse media checks, on the officers and UBOs of its B2B business partners.

In addition to these measures, the Company considers the duration of the business relationship, whether the partner or its officers/UBOs have been subject to any regulatory or enforcement actions, the internal policies and procedures of the B2B partner, the payment methods used for transactions with Digitain and the markets or jurisdictions the partner intends to target. Special attention is also given to whether online gaming is legal within those jurisdictions.

Geographical Risk: This pertains to the areas and jurisdictions in which the Company operates, as well as the locations of its B2B business partners. These regions may, at times, present an elevated risk for money

laundering and terrorist financing, as identified by the FATF and other credible organizations such as Transparency International. Clients from or linked to these high-risk countries will be classified by Digitain as 'high risk':

(a) Any country subject to sanctions, embargoes, or similar measures imposed by international organizations, such as the United Nations Security Council. Additionally, countries under sanctions or measures that may not be universally recognized, but whose significance or nature of the sanctions warrants recognition, may be considered high risk by Digitain.

(b) Any country identified by credible sources as providing support for terrorist activities or hosting designated terrorist organizations.

(c) Any country known to be a tax haven, a source of narcotics, or involved in other significant criminal activities.

(d) Any country flagged by the FATF as non-cooperative in the fight against money laundering or terrorist financing, or that is subject to a FATF statement.

(e) Any country identified by credible sources as lacking appropriate money laundering or terrorist financing laws and regulations or exhibiting high levels of corruption.

(f) Digitain refrains from conducting business or providing services to any individual or entity in countries that are subject to comprehensive international sanctions or excluded due to regulatory restrictions.

Service Provision Risk: This risk arises from the nature of the services the Company provides. Its B2B business partners operate B2C online gaming platforms that may be exploited for money laundering, terrorism financing, fraud and other criminal activities.

To mitigate this risk, Digitain ensures that its business partners comply with rigorous anti-money laundering (AML) and fraud prevention policies, alongside other internal procedures that align with their business models and operations. The company verifies the authenticity of any licenses, approvals and certifications provided by potential business partners and continuously monitors the delivery channels (websites) through which its partners interact with end consumers. Furthermore, Digitain requires its business partners to contractually commit to training their staff to identify and report suspicious activities related to money laundering, terrorism financing, fraud and other illegal acts. The company also reserves the right to refuse any new business relationships or to review and terminate existing relationships at its sole discretion.

Additionally, Digitain conducts extensive due diligence on third-party products and services before onboarding them. This includes evaluating the appropriateness of such tools and services for their intended purpose. The company imposes strict technical standards and enters into service-level agreements with its service providers to ensure continuity of service and the availability of necessary support.

Internal Risk: This risk arises from employees (e.g., human error) and third-party products and services used by Digitain in conducting its business operations.

To address this, Digitain undertakes thorough screening of potential employees, including background checks, identity verification and reference checks, as well as running candidate information through PEP and sanction screening lists. Once employed, all employees undergo comprehensive training in both their areas of expertise and in anti-money laundering and terrorism financing procedures.

In addition, Digitain implements strict access controls on the dissemination of information within the Company, ensuring that it is shared on a need-to-know basis. The Company also ensures sufficient staffing levels to perform tasks efficiently, reducing the risk of human error and conducts regular performance assessments to maintain high standards of operational effectiveness.

12. Training and Awareness

To uphold high levels of compliance and awareness within the iGaming sector, Digitain is committed to providing regular, comprehensive training to all employees on Anti-Money Laundering (AML), Counter-Financing of Terrorism (CFT) and Financing of Proliferation (FP) regulations. This training will focus on key areas such as risk identification, reporting obligations and adherence to internal policies and procedures. This ensures that all staff members are well-equipped with the necessary knowledge to identify and respond to potential risks and comply with regulatory requirements. Continuous training will also be provided to keep employees updated on evolving compliance obligations and emerging risks within the sector. By fostering a culture of compliance through ongoing education, Digitain ensures that its workforce remains vigilant and capable of maintaining the highest standards of regulatory compliance.

13. Record Keeping and Documentation

Digitain will maintain detailed records of all customer identification data, transaction histories, risk assessments, reports of unusual transactions and employee training for a minimum of five (5) years, in compliance with regulatory requirements. In addition, all policies, procedures, risk assessments and internal audits will be formally documented, reviewed and approved by Digitain's Board of Directors. These records will be made available to the Curaçao Gaming Control Board (GCB) upon request, ensuring transparency and full regulatory compliance within the iGaming sector.

14. Audit and Internal Controls

To ensure the ongoing effectiveness of its AML/CFT/FP program and adherence to applicable regulations, Digitain will conduct regular internal audits to assess the strength and efficiency of its compliance measures.

15. Digitain Statement

Digitain is dedicated to upholding the highest standards of vigilance in preventing money laundering, terrorism financing and other financial crimes. By implementing a comprehensive, risk-based approach to due diligence, partner screening and ongoing monitoring, we ensure strict compliance with all applicable regulatory requirements. Our commitment to these measures is essential to maintaining the integrity and reputation of the business, ensuring that we operate securely and in full compliance at all times.

Digitain is fully committed to upholding the highest standards of integrity and regulatory compliance across all aspects of its operations within the iGaming sector. As part of this commitment, we have implemented comprehensive policies and procedures designed to prevent the misuse of our facilities, products and services for money laundering, terrorist financing and the proliferation of weapons of mass destruction.

We strictly adhere to all relevant laws, regulations and industry best practices to ensure our platforms and services are not exploited for illicit activities. This includes conducting thorough due diligence on our business partners and customers, monitoring for suspicious activity and ensuring that our employees, partners and third-party service providers are well-trained and fully understand their responsibilities in maintaining compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) obligations.

Digitain is dedicated to fostering a secure, transparent and legally compliant environment for all stakeholders. We remain vigilant in our efforts to prevent the exploitation of our services for criminal purposes and will continue to take all necessary measures to protect the integrity of our business operations. This policy reflects our unwavering commitment to supporting the global fight against financial crime and ensuring the continued trust and safety of our partners and customers.