

Special Consolidator B.V.

POLICY
On Combating Money Laundering
and
Terrorism Financing

Special Consolidator B.V.

VERSION CONTROL..... 2

INTRODUCTION AND SCOPE.....3

1. RISK BASED APPROACH TO AML, CTF and CPF.....4

2. CUSTOMER DUE DILIGENCE (CDD).....5

 2.1. Stages of CDD.....6

 2.2. Enhanced Due Diligence..... 7

 A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting due to being considered more vulnerable to bribery and corruption.....8

 2.3. Ongoing Monitoring, Periodic and Event-Driven Reviews of Customer Due Diligence..... 9

 2.4. Reliance on Third Parties for Customer Due Diligence..... 10

3. NOMINATED OFFICER..... 11

4. SENIOR MANAGEMENT..... 12

 4.1. Escalation to Senior Management..... 12

5. RECORD KEEPING..... 12

6. REPORTING OF SUSPICIOUS ACTIVITY..... 13

7. EMPLOYEE DUE DILIGENCE AND SCREENING..... 13

8. STAFF TRAINING..... 14

9. INDEPENDENT REVIEW..... 15

10. POLICY REVIEW..... 15

Special Consolidator B.V.

VERSION CONTROL

VERSION NUMBER	DATE	APPROVED BY
1.0	25.07.2025	Director

Special Consolidator B.V.

INTRODUCTION AND SCOPE

Special Consolidator B.V. (hereinafter referred as “Special Consolidator” or “We” or “Us”) is committed to preventing its products and services from being used to launder money, or assist in the financing of terrorism.

Money Laundering (ML) can cover a wide range of circumstances, include trying to turn money raised through criminal activity into “clean” money, possessing or transferring the benefit of acquisitive crimes such as theft and fraud, possessing or transferring stolen goods, being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property, and criminals investing the proceeds of their crimes. It also includes spending the proceeds of crime, as opposed to merely concealing or converting it.

Terrorist Financing (TF) is the provision or collection of funds, by any means, directly or indirectly with the intention that they should be used or in the knowledge that they are to be used in full or in part in order to carry out any terrorism offences. The fundamental difference between terrorist financing and money laundering lies in the origin of the funds. Terrorist financing involves the use of funds for illegal political purposes, but the money is not necessarily derived from illicit sources. In contrast, money laundering always involves funds that originate from criminal activity.

The purpose of this policy is to outline the processes and procedures established to prevent and mitigate the risks of money laundering and the financing of criminal activities.

To achieve this goal, the policy covers the following key areas:

- Risk - Based approach to AML, CFT and CFP
- Customer Due Diligence (CDD)
- Enhanced Due Diligence (EDD)
- Ongoing Monitoring
- Nominated Officer
- Senior Management
- Employee screening and due diligence
- Employee training
- Recording & Reporting, etc.

This Policy has been designed to ensure adherence to, among others, the following legislation and regulations:

- National Ordinance on Games of Chance;
- Regulations for the Combating of AML, CTF and Proliferation of weapons of mass destruction applicable to Curacao casinos and providers of other online games (2025);

Special Consolidator B.V.

- Regulations of AML and CFT (2016);
- Other applicable legislation.

This Policy is mandatory across the entire Company. Where the requirements of this Policy conflict with local laws or regulations, the applicable jurisdictional requirements must take precedence, and the business must document such instances accordingly.

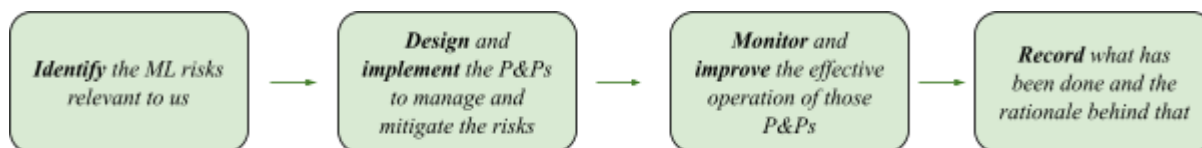
Special Consolidator maintains a zero-tolerance stance toward breaches of financial crime legislation and regulations. In line with this commitment and its defined risk appetite, this Policy outlines a clear set of standards and requirements that the business must follow.

No part of the Company, nor any individual acting on its behalf, may take any action intended to circumvent or undermine the purpose of this Policy. This Policy should be read in conjunction with all relevant supporting documentation and other applicable Policies and Procedures (P&Ps).

1. RISK BASED APPROACH TO AML, CTF and CPF

Special Consolidator has adopted a risk-based approach to AML, CTF and CPF with the aim of managing and mitigating money laundering risks in a proportionate way.

A risk-based approach involves a number of steps to put in place the most proportionate way to manage and mitigate the risks faced by Special Consolidator. We will use the following approach.



The risk assessment must be appropriate and must be reviewed as necessary in light of any changes in circumstances, including the introduction of new products, business practices or technology, changes in the customer's demographic, etc.

In general, risk is based on the following categories, though there may be some overlap between them:

- Customer risk
- Country or geographic risk
- Product and service risk
- Transaction risk
- Third-party service risk

Special Consolidator B.V.

Customer risk factors may include:

- The Customer being based in a geographical area of high risk ([FATF List of High-Risk and other monitored jurisdictions](#));
- The Customer is a company that has nominee shareholders;
- The Customer is a business that is cash intensive;
- The Corporate structure of the Customer is unusual or excessively complex given the nature of the company's business, etc.

Country or geographic risk factors may include:

- Countries that are included in the [FATF list of High-Risk and other monitored jurisdictions](#);
- Countries providing funding or support for terrorism;
- Countries with a high risk of money laundering, according to [Basel AML Index](#), etc.

Product, Service and Transaction risk factors may include:

- The software that allows a high level of anonymity or limited identity verification for end-users;
- The operator has significant autonomy to disable or bypass built-in AML/monitoring tools;
- The payments are received from unknown or unassociated parties, etc.

Third party risk factors may include:

- The third party operating without a license (if required);
- The third party accessing to customer data or financial transactions without contractual safeguards or compliance obligations;
- The relationship lacks transparency on the ownership, structure, or business activities of the third party, etc.

2. CUSTOMER DUE DILIGENCE (CDD)

Our Customer due diligence (CDD) or Know Your Business (KYB) process helps us to collect information on a potential customer to ensure that all stages of the business and all relevant stakeholders have a clear understanding of who the customer is and the intended nature of their business, as well as to assess any risk they may bring to business.

By performing thorough due diligence, we mitigate the risk of involvement in unlawful activities, safeguard the integrity of our products and services, and maintain trust with our clients, customers, and stakeholders. Additionally, we comply with local and international

Special Consolidator B.V.

regulations, including those set forth by regulatory authorities of the applicable jurisdiction, which require the implementation of such measures.

Our customers are primarily other business entities, such as Gaming website operators (B2C), Gaming software providers and/or resellers, distributors (B2B), and other related service providers (3rd party vendors, etc.).

These businesses utilize our gaming software and related products to offer online gaming services to their own end-users or partners. As part of our CDD process, we focus on conducting due diligence on these business customers to verify their legitimacy, good standing and regulatory compliance.

2.1. Stages of CDD

As a first stage, a CDD check should be conducted before establishing any business relationship with potential customers/partners. When entering into a new business relationship, we begin with Basic Due Diligence. If there are any red flags or higher risks, we will perform Enhanced Due Diligence to assess the potential risks further.

As a second stage, to ensure continued compliance and minimize risk exposure, we periodically conduct updates and reviews, especially if there are changes in business operations, ownership structure, or jurisdictional regulations. Based on industry practices and a general understanding of various regulatory requirements, ongoing CDD is typically conducted every 6 months or annually following the onboarding of a customer. While the company prefers to conduct ongoing due diligence every 6 months, especially when the company undergoes audits or other regulatory checks, the general approach remains to perform it annually.

As a third stage, if a regulatory violation or other significant event occurs, we will perform additional checks to reassess any risks associated with the customer and ensure they are still compliant and remain low-risk. This Post-Incident DD is the least likely scenario.

To establish a “customer risk”, one of the below three levels of DD may be performed proportionally to the increasing level of risk identified:

- Simplified Due Diligence - relaxed procedures used for low risk customers
- Standard Due Diligence - standard procedure used for medium/average risk customers
- Enhanced Due Diligence - strengthened procedures used for high-risk customers.

Below is the table of scenarios for each CDD level:

Criteria	Simplified DD	Standard DD	Enhanced DD
----------	---------------	-------------	-------------

Special Consolidator B.V.

License	Holds a valid gaming license from a respected jurisdiction	License is close to expiry and/or regulatory environment may be evolving	Not licensed/expired and no proof of having applied for the new
Legal claims	No news on legal claims	News with positive resolution	News with negative or no resolution
Company Structure	Simple structure and reputable jurisdiction	Medium structure and semi-reputable jurisdiction	Difficult structure and non-reputable jurisdiction

The list below outlines the general framework of information typically requested as part of our due diligence process. This provides a high-level overview of the categories of information we may collect.

Please note that further detail - including the specific documents required - is set out in our internal procedures, particularly the Company's Customer CDD Guide, which serves as a reference point for onboarding and monitoring processes.

The general categories of information may include:

- Basic corporate information (e.g. company name, registration number, registered address, etc.);
- Details of the company's ownership structure;
- Identification documents and verification of the Ultimate Beneficial Owner(s) (UBOs);
- Identification and verification of directors and key management personnel;
- Description of the nature of the business;
- Information on the intended business relationship;
- Licensing or regulatory information, if applicable;
- Details of any third-party service providers or business partners involved;
- Information regarding the geographical areas of operation;

The CDD information and documentation may be retained and used for ongoing monitoring and periodic review purposes, in line with our internal compliance procedures and legal obligations.

2.2. Enhanced Due Diligence

We must apply EDD measures where there is:

- A material change in the risk rating of the Customer or where a high risk red flag is identified;

Special Consolidator B.V.

- A doubt regarding a veracity of the Customer information provided, including their identity;
- A suspicion on ML, TF, Fraud, etc.

EDD measures applied shall include

- Performing checks on third party databases;
- Conducting open source checks, such as social media websites;
- Checking the relevant corporate documentation against the data available from relevant registries;
- Requesting additional information;
- Increasing the degree and nature of monitoring of the business relationship and activities, etc.

In line with our risk-based approach to Customer Due Diligence, certain categories of customers—such as politically exposed persons (PEPs)—require enhanced scrutiny due to the elevated risk they may pose.

A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting due to being considered more vulnerable to bribery and corruption.

Therefore, full enhanced due diligence must be conducted upon any identified PEPs. The Company does not distinguish between foreign and domestic PEPs, all are considered high risk. A PEP that no longer holds their prominent public role will also be deemed high risk.

A PEP is defined as a natural person who is or entrusted with prominent public functions, including:

- A head of state, head of government, minister or deputy or assistant minister;
- A senior government official;
- A Member of Parliament (MP);
- A senior politician;
- An important political party official;
- A senior judicial official;
- A member of a court of auditors or the board of a central bank;
- An ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
- A high-ranking officer in an armed force;
- A senior member of an administrative, management or supervisory body of a State-owned enterprise;
- A senior official of an international entity or organization.

A PEP also includes family members and close associates of the above, including:

- A spouse;

Special Consolidator B.V.

- A partner considered by national law as equivalent to a spouse;
- Other known close personal relationships such as a partner, boyfriend or girlfriend;
- A child;
- A spouse or partner of a child;
- A brother or sister (including a half-brother or half-sister);
- A spouse or partner of a brother or sister;
- A parent;
- A parent-in-law;
- A grandparent;
- A grandchild;
- A joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with a PEP;
- The sole beneficial owner of a legal person or legal arrangement known to have been set up for the benefit of a PEP;
- A beneficiary of a legal arrangement of which a PEP is a beneficial owner or beneficiary;
- A person in a position to conduct substantial financial transactions on behalf of a PEP.

When the Company identifies a relationship with a Politically Exposed Person (PEP), it must:

- Obtain senior management approval before establishing (or continuing, in the case of existing customers) such a business relationship;
- Clearly document the rationale for initiating, continuing, or terminating the relationship with the PEP; and
- Apply enhanced ongoing monitoring of the business relationship.

For at least 12 months after a PEP ceases to hold a prominent public function, the Company should continue to assess the risk associated with that individual and apply enhanced measures where appropriate.

2.3. Ongoing Monitoring, Periodic and Event-Driven Reviews of Customer Due Diligence

As part of our Customer Due Diligence (CDD) obligations, we conduct ongoing monitoring of all business relationships to ensure customer information remains current and relevant. This includes regular checks to verify that the customer's activity aligns with the expected profile and risk level.

In addition to ongoing monitoring, the Company performs:

- Periodic reviews at set intervals based on the customer's risk rating and

Special Consolidator B.V.

- Event-driven reviews triggered by specific circumstances, such as a change in ownership, unusual transaction behavior, or negative media coverage.

2.4. Reliance on Third Parties for Customer Due Diligence

Where Special Consolidator relies on agents or third parties to carry out elements of the Customer Due Diligence process, it is important to note that the ultimate responsibility for ensuring compliance with all applicable CDD requirements remains with the Special Consolidator .

Accordingly, Special Consolidator must ensure the following:

- Appropriate due diligence is carried out to assess the suitability of the agent or third party;
- Special Consolidator obtains assurances that the relevant documentation can and will be provided without delay when requested;
- The respective roles, obligations, and responsibilities of Special Consolidator and the third party are clearly defined and documented in a formal agreement.

Reliance on third parties for certain CDD elements may not always be appropriate, particularly where the outsourced party is not in a position to make final onboarding decisions, which should remain the responsibility of the Special Consolidator.

Reliance on Group, Subsidiary, or Affiliated Entities

In the course of conducting Customer Due Diligence and related AML/CFT processes, Special Consolidator may, where appropriate, rely on other entities within its group structure, including subsidiaries or affiliated companies. Such reliance is permissible only under the following conditions:

- The related entity must apply AML/CFT policies and procedures that are equivalent in standard to those outlined in this Policy and in the applicable regulations;
- The related entity must be subject to regulation or supervision by a competent authority in a jurisdiction that applies AML/CFT standards equivalent to those required under the applicable law or these internal standards.

It is important to note that any reliance on a group, subsidiary, or affiliated entity does not transfer the Company's responsibility for regulatory compliance. The ultimate responsibility for ensuring full compliance with CDD and decision-making obligations remains with the Company at all times.

Special Consolidator B.V.

3. NOMINATED OFFICER

Special Consolidator's Senior Management must appoint a Nominated Officer, commonly referred to as the Money Laundering Reporting Officer (MLRO) and/or Compliance Officer, who is responsible for overseeing the implementation of our anti-financial crime measures. The Nominated Officer acts as the central point of contact for all internal and external reporting of suspicious activity and ensures that we comply with all applicable AML/CTF laws and regulations.

Until such time as a dedicated Nominated Officer is formally appointed, the responsibilities of this role may be fulfilled by suitably qualified staff within the Group or an affiliated entity, or through outsourcing to an appropriately experienced third party.

The Nominated Officer must have the appropriate level of seniority, knowledge, and independence to carry out their duties effectively, which include:

- Receiving and evaluating internal suspicious activity reports;
- Escalating concerns to the relevant authorities where appropriate;
- Maintaining records of investigations and reports submitted;
- Ensuring ongoing compliance with internal policies and regulatory obligations;
- Liaising with regulators, law enforcement, and other authorities as necessary;
- Staff training to be aware of the approved policies and procedures in this area and the reporting structure;
- Carrying out any other duties as required by law, regulation, or internal governance in connection with their role.

All employees have a duty to:

- Stay alert to potential signs of money laundering activity;
- Report any suspicions or knowledge of such activity to the Nominated Officer without delay;
- Fully adhere to the Company's policies and procedures, including those related to customer identification, ongoing monitoring, record-keeping, and reporting obligations.

4. SENIOR MANAGEMENT

Senior Management should support the MLRO and encourage active cooperation from all Staff.

Special Consolidator B.V.

Senior Management should ensure the Special Consolidator's policies and procedures are clearly communicated to Staff by the Nominated Officer.

Senior Management will ensure the mechanisms are in place, including an independent audit when appropriate, to ensure the policies and procedures are carried out effectively, weaknesses are identified and improvements are made where necessary by the Nominated Officer.

Any Senior Management decisions should be documented to ensure there is evidence of all decision-making processes and an audit trail.

4.1. Escalation to Senior Management

In situations where significant risks are identified, and the Nominated Officer considers it necessary, there should be a clear and structured process to escalate such matters to Senior Management for joint decision-making. To support this, the Company should have formal governance procedures that enable the escalation of high-risk or complex cases to either the Board of Directors or a designated Risk Committee composed of senior managers and the Nominated Officer. These forums must be properly constituted, with documented meeting minutes and the use of formal assessment tools.

5. RECORD KEEPING

Keeping proper records is important to make sure there is a clear audit trail, and to allow the Company to monitor situations, revisit decisions, and make better judgments in the future. Records also help us stay compliant with regulatory requirements and respond to any internal or external reviews.

Special Consolidator will keep records related to:

- Customer Due Diligence (CDD) decisions and documents used to support those decisions;
- Reviews or updates of CDD, whether done regularly or due to specific events;
- Reports and escalations made by the Nominated Officer to senior management or the Board;
- Communication between the Nominated Officer and any regulatory authority;
- Employee training, including who was trained, when, and what training was provided;
- Any documents supporting our business relationships and risk decisions;
- Internal communications related to financial crime risk;

Special Consolidator B.V.

- Any other records that are needed to support our work or show we are meeting our legal obligations.

All records must be stored securely and be easy to find if needed for internal checks or regulator requests.

6. REPORTING OF SUSPICIOUS ACTIVITY

Any employee who knows, suspects, or has reasonable grounds to believe that a customer is involved in money laundering or terrorist financing must escalate the matter internally to the Nominated Officer without delay.

- The escalation must be properly documented and recorded;
- Discussions about the suspicion should be limited only to those who need to know - primarily the Nominated Officer - to avoid the risk of *tipping off*;
- Under no circumstances should the customer be informed that a suspicious activity report (SAR) is being considered or filed.

If necessary, the Nominated Officer may consult with senior management. However, it is solely the Nominated Officer's responsibility to decide whether to file an external report with the relevant regulatory authority, always ensuring that any decision is made in full compliance with applicable laws and regulations.

7. EMPLOYEE DUE DILIGENCE AND SCREENING

Special Consolidator applies appropriate, risk-based measures to check the integrity of prospective employees, especially those who may be in a position to facilitate money laundering or other financial crime. This includes deciding whether and how to screen a person before hiring, and whether re-screening is needed if the person is promoted or moved to a higher-risk role. These checks help us ensure that people in key roles are trustworthy and suitable for their position.

We carry out steps such as:

- Requesting and verifying references;
- Reviewing previous employment and comparing it against the CV;
- Checking and retaining copies of relevant qualifications;
- Asking for information about any previous criminal convictions or regulatory actions.

Special Consolidator B.V.

Special Consolidator must have a system in place to address situations where an employee, without reasonable excuse, fails to follow internal systems, controls, or procedures.

8. STAFF TRAINING

Inadequately trained staff may lack the knowledge and skills needed to ensure compliance with applicable laws and regulations, which poses a serious risk to the Company. To manage this risk, we are committed to providing comprehensive, effective, and relevant training to our employees.

Training will cover at least the following areas:

- Overview of the Company and the licenses it holds;
- Summary of applicable laws and regulations;
- Core principles of Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF);
- Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and ongoing monitoring;
- Identifying and reporting suspicious activity;
- Internal policies and procedures;
- Responsibilities of staff in relation to financial crime prevention.

More specific and in-depth training may be arranged, including sessions delivered by external experts, for roles such as:

- Money Laundering Reporting Officer (MLRO) and Compliance team;
- Fraud prevention staff;
- IT and security teams;
- Senior management.

Training must be delivered on an ongoing basis—such as when there are regulatory changes—and refreshed annually to maintain up-to-date knowledge.

Special Consolidator will:

- Keep records of all training sessions to track attendance and plan future sessions;
- Ask for staff feedback after each session to assess effectiveness;
- Assign overall responsibility for training design, delivery, and review to the Nominated Officer.

9. INDEPENDENT REVIEW

Special Consolidator B.V.

Special Consolidator may, where deemed appropriate, engage an independent review or audit to assess the effectiveness of its systems, controls, and overall compliance framework in preventing financial crime.

The audit must be independent—meaning it must be conducted by individuals who are not involved in the organisation’s day-to-day compliance functions. The scope and results of the review must be clearly documented.

The frequency of such reviews should reflect the nature, size, and complexity of the Company’s business, as well as the level and type of money laundering or terrorism financing risks it may face. However, an independent review must be conducted at least once every two years.

10. POLICY REVIEW

This policy shall be reviewed and updated whenever there are significant changes in relevant laws, regulations, or business operations that affect its content. In any case, a full review must be conducted at least annually to ensure continued effectiveness and compliance.

Signed by:  E9C1A4A3F74E4ED...	DocuSigned by:  98427330719E4A1...
---	---

Director OBO Xecutive Corporate Management B.V
Special Consolidator