

AML Policy (CW)

Anti-Money Laundering and Counter Terrorist Financing Policy

Document Information

Document Title	Anti-Money Laundering and Counter Terrorist Financing Policy
Version Number & summary of updates	
1.0	Original
1.1	Updated formatting Broadened scope as a group policy Broadened scope of services to include provision of payment processing services
1.2	Addition of adequate screening/ verification prior to hiring employees
1.3	Updates to sanctions list
1.4	Comprehensive rewrite to align with Curaçao AML/CFT/CFP Regulations: new structure; NAF 4,000 CDD gating & 30-day rule; NAF 5,000 objective UTRs & timelines; formal RBA (BRA/CAP/CRA); EDD/PEP controls; SDD guardrails; sanctions/HR-country & PF controls; MLRO role; training/screening; independent audit; record-keeping (≥5y); new tech & third-party reliance; QA/MI; breaches/tipping-off; appendices; typo fixes (e.g., "sanctions")

Section 1 — Document Control & Governance

1.1 Document Owner

This policy is owned by the **Compliance Officer / MLRO** ("CO/MLRO"). The CO/MLRO is responsible for maintaining the AML/CFT/CFP program, verifying compliance with laws and policies, coordinating internal/external unusual-transaction reporting, employee training, and management reporting to the Board. Deputies may act in the CO/MLRO's absence.

1.2 Version Control & Review Cycle

- **Version:** 1.4 (supersedes 1.3)
- **Effective date:** 01.09.2025
- **Change log:** Maintained in the Document Information table.
- **Review frequency:** **Annually**, or **earlier on material change** in business model, products, delivery channels, risk exposure, or regulation. The CO/MLRO proposes updates; the Board approves.

1.3 Approvals & Governance

- **Prepared by:** CO/MLRO
- **Reviewed by:** Senior Management
- **Approved by:** Board of Directors of Slotbox N.V.
- **Evidence:** Signed Board minute/resolution and policy version archived with the policy register.

1.4 Scope & Applicability

This policy applies to Slotbox N.V. and any subsidiary or contracted party facilitating online casino/games of chance under Curaçao oversight or otherwise processing player activity covered by this policy. Where local law imposes stricter standards, those prevail.

1.5 Regulatory Basis & Alignment

This policy implements Curaçao's **AML/CFT/CFP Regulations for casinos** and relevant FATF Recommendations (incl. CDD, record-keeping, PEPs, new technologies, reliance on third parties, internal controls, higher-risk countries, SAR/UTR, and tipping-off prohibitions).

1.6 Related Areas

- Business Risk Assessment (BRA) & methodology.
- Customer Acceptance Policy (CAP) & Customer Risk Assessment (CRA).
- CDD/EDD/SDD Procedures; Sanctions & PEP Screening SOP.
- Unusual Transaction Reporting (UTR) SOP (goAML portal), internal SAR form.

- Employee Screening & Training Plan (with training records).
- AML Program Audit plan/report (annual).
- Record-Keeping & Data Retention Standard (≥5 years; reconstructability).

1.7 Distribution & Accessibility

The approved policy is published on the compliance policy register, communicated to all relevant employees and contractors, and made available to the GCB/FIU Curaçao upon request. (Policies must be Board-approved and communicated to staff.)

1.8 Exceptions & Change Management

Any temporary deviation requires **written approval from the CO/MLRO** and **notification to the Board** as appropriate. All exceptions and remediations are logged

Section 2 — Purpose, Scope & Legal/Regulatory Basis

2.1 Purpose

This policy establishes the Slotbox AML/CFT/CFP framework for online casino operations, ensuring we prevent, detect, and report money laundering, terrorist financing, and proliferation financing, and that our internal controls (CDD/EDD/SDD, ongoing monitoring, sanctions/PEP screening, UTR reporting, training, record-keeping, and independent audit) meet Curaçao requirements and FATF Recommendations.

2.2 Scope

Entities. This policy applies to Slotbox operating online games of chance under Curaçao oversight, and any related party processing player activity within scope.

Products & services. Real-money online casino products and related services that may present ML/TF/PF risk.

Delivery channels. Web, mobile, and any future channels/new technologies (subject to prior risk assessment under the RBA).

Customers. All players (natural persons) and, where applicable, corporate applicants; anonymous or fictitious accounts are prohibited.

2.3 Legal/Regulatory Basis

This policy implements the **AML/CFT/CFP Regulations applicable to Curaçao casinos**

2.4 Key Regulatory Thresholds & Operating Rules

- **CDD trigger:** Apply CDD when a player engages in financial transactions $\geq$ **NAf 4,000** (including cumulative/related transactions), on suspicion of ML/TF, or when there are doubts about prior identification data. At account opening, collect personal details and conduct sanctions screening at minimum.
- **Use of account while CDD is in progress:** Players may use the account while CDD is carried out; however, **once NAf 4,000 is reached, no further deposits or withdrawals are allowed** until required CDD is completed. Threshold is **calculated daily** taking all deposits and withdrawals into account since the relationship start.
- **30-day rule:** If required CDD documentation is not received **within 30 days** of reaching NAf 4,000, the **business relationship must be terminated**, and an **unusual transaction report** must be filed with the FIU where a presumption of ML exists.
- **UTR (Unusual Transaction Reporting) objective indicators:** Report via goAML when any of the following occur: a transaction, bank transaction, sale of chips/credits, or prize payment $\geq$ NAf 5,000; also if the person is on a UN/EU sanctions list or where ML/TF was reported to authorities.
- **UTR process & timelines: Objective-indicator** UTRs within **48 hours of the transaction**. For **subjective indicators**, internal report to the CO $\leq$ **24 hours**; the CO has **10 working days** to research and, if ML/TF is presumed, must report to the FIU within **48 hours**. Submissions are via the **FIU Curaçao goAML portal** and **in English**.
- **Ongoing monitoring:** Keep CDD information current, link multiple accounts, scrutinize activity against risk profile, and obtain SoF/SoW as needed; escalate UTRs where appropriate.
- **Record-keeping:** Maintain **transaction** and **CDD** records for **at least 5 years** (after relationship end/occasional transaction), enabling reconstruction of individual transactions.

2.5 Risk-Based Approach (RBA) linkage

Our Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) drive control intensity (SDD/CDD/EDD) across player, country, product, service, and delivery-channel risk factors. The BRA is documented, Board-approved, reviewed on change (or annually) with sources, methodology, and L/M/H rationale recorded; the CAP sets higher-risk player types, risk indicators, and monitoring levels.

2.6 Interaction with Group/Local Requirements

Where another applicable jurisdiction imposes stricter AML/CFT requirements, we apply the stricter standard. This policy is read together with the BRA, CAP/CRA, CDD/EDD/SDD Procedures, Sanctions/PEP SOP, UTR SOP, Training Plan, and Record-Keeping Standard referenced in Section 1.6.

Section 3 Risk-Based Approach (RBA, BRA, CAP/CRA)

3.1 RBA Overview

We apply a **risk-based approach** so that preventive measures are **commensurate with the ML/TF/PF risks identified**. This includes: (i) assessing risk; (ii) implementing risk-mitigating policies, procedures, and controls; (iii) monitoring and improving those controls; and (iv) documenting our assessments. We consider player, country, product, service, and delivery-channel risk factors and the relevant National Risk Assessment.

3.2 Business Risk Assessment (BRA)

- **Purpose.** Identify how our **products/services, payment methods, countries, delivery channels, and technologies** could be used for ML/TF, define **risk appetite**, and set the AML/CFT program controls accordingly.
- **Governance & cadence.** The BRA is **Board-approved, revised on environmental or business changes**, and **reviewed at least annually** if no changes arise.
- **Methodology & workpapers.** We document (a) the methodology, (b) the rationale for **Low/Medium/High** ratings, (c) outcomes and residual risks, and (d) **sources of information** used (including NRA, internal MI, and external typologies).

- **Outputs.** The BRA drives our **AML/CFT program** (Sections 4–11), including thresholds, monitoring intensity, training scope, and the independent audit plan.

3.3 Customer Acceptance Policy (CAP) & Customer Risk Assessment (CRA)

- **Purpose.** Determine the **player-level risk** at onboarding and throughout the relationship and set the **level of CDD (SDD/standard/EDD)** and monitoring required.
- **Risk factors.** Player profile/behavior, **country** exposure, **product/service** usage, **delivery channels/technologies**, PEP status, and **sanctions screening** outcomes.
- **CAP contents.** Defines **higher-risk player types**, **risk indicators** with L/M/H scales, and the **corresponding CDD & ongoing-monitoring level**. Explicit consideration of **PEPs** and **sanctions** is required. Anonymous or fictitious accounts are prohibited.
- **CRA timing.** CRA is performed at onboarding (with minimum personal details + sanctions check) and updated **on trigger events** (e.g., activity inconsistent with profile, material KYC changes) or **periodically** by risk tier.

3.4 Risk Scoring & Control Application Matrix

We map CRA scores to controls as follows (minimum standards):

- **Low Risk (SDD may apply)**

Reduced update frequency and monitoring **proportionate to lower risk**; identity/BO verification can be sequenced **after** relationship start if justified by risk and never where suspicion/higher-risk exists.

- **Medium Risk (Standard CDD)**

Full CDD (ID&V, sanctions check, purpose/intended nature), ongoing monitoring with scenario alerts; obtain **SoF** where activity deviates from profile.

- **High Risk (EDD)**

Senior management approval to onboard/continue; **enhanced monitoring**, **more frequent data refresh**, **SoF/SoW** with independent evidence as needed;

consider **first payment from an account in player's name** at a CDD-standard bank.

3.5 Ongoing Monitoring & Risk Updates

- Keep CDD data **current**; obtain fresh documents on expiry; question inconsistencies; **scrutinize transactions** vs. risk profile; obtain **SoF/SoW** where warranted. **Link all accounts** held by the same player and detect multi-accounting/third-party identity use.
- When activity is not in line with expectations: establish SoF and/or **revise the risk profile**; assess for **Unusual Transaction Reporting** to the FIU (see Section 7).

3.6 Triggers to Re-perform CRA / Escalate Controls

- Hitting monetary or behavioral **scenario thresholds**; repeated values **just under objective indicators**; rapid deposit/withdrawal cycling; use of multiple payment instruments; country risk changes; **PEP hits/changes**; sanctions alerts; or material changes in product/channel use.

3.7 New Technologies & Delivery Channels

Before launching new products, payment rails, or delivery channels, perform a **pre-implementation risk assessment** and update the BRA/CAP/CRA and control set accordingly (including monitoring scenarios and staff training).

3.8 Roles & Reporting

The **CO/MLRO** owns the BRA and CAP/CRA frameworks, ensures periodic **management information** to Senior Management and the **Board**, and maintains auditable workpapers supporting ratings, changes, and residual risks.

Section 4 — Customer Due Diligence (CDD)

4.1 CDD objectives

Implement identification, verification, sanctions/PEP screening, CRA, and ongoing monitoring sufficient to ensure we know the player and our products are not used to launder money, finance terrorism, or PF. Anonymous or fictitious accounts are prohibited.

4.2 When CDD is required

We perform CDD:

- when a player engages in financial transactions **≥ NAf 4,000**, including **occasional transactions** above the equivalent of NAf 4,000, or a **series of related transactions**;
- on **suspicion of ML/TF**; or
- where we **doubt** the adequacy/veracity of prior identification data.

4.3 Timing & use of account

- At **account opening**, we collect **minimum personal details** and conduct **sanctions screening**. Players **may use** the gaming account while CDD is being carried out.
- Once the **NAf 4,000** threshold is reached, **no further deposits or withdrawals** are allowed **until CDD measures are completed**.
- The **threshold is calculated daily**, taking **all deposits and withdrawals** into account since relationship start.
- If required documents are **not received within 30 days** of reaching NAf 4,000, we **terminate the relationship** and file a **UTR** if ML/TF is presumed.

4.4 Standard CDD measures

We complete the following (commensurate with risk):

1. **Identify the player** (collect personal details): **name, permanent residential address, date and place of birth, nationality, and an identity/ID number**.
2. **Sanctions screening** at onboarding and on a risk-sensitive basis thereafter (e.g., EU and OFAC lists).
3. **Verify identity** using **reliable, independent** sources (valid, unexpired government photo ID: **passport, national ID card, or driver's licence**).
4. **Verify address** (≤ 6 months old): **bank statement, utility bill, government correspondence, lease, or direct contact** (phone/letter/email) as appropriate.
5. **Other verification signals** (risk-based): **geolocation, IP, funding-method data, biometric/tech controls**; apply additional steps where inconsistencies

are detected.

6. **Beneficial owner (BO) check:** for player accounts, we obtain a **self-declaration in T&Cs (tick-box “registering on own behalf”)**; BO situations are **rare** but must be identified where applicable.
7. **Purpose/intended nature:** in gaming the purpose is usually **self-evident**; nonetheless, maintain a **player profile** and, where necessary, collect **SoW** information (declaration may suffice at low risk; otherwise independent evidence).
8. **Customer Risk Assessment & PEP screening** at onboarding and on triggers thereafter.

4.5 Ongoing monitoring

- Keep CDD information **up-to-date**; refresh ID/addresses on expiry; question inconsistencies.
- **Scrutinize transactions** against player profile/risk; obtain **SoF/SoW** where warranted.
- **Link all accounts** held by the same player; detect multi-accounting and third-party identities.
- When activity deviates from expectations, **revise risk profile** and assess for **UTR**.

4.6 Inability to complete CDD

If we cannot obtain/verify required CDD:

- **Do not** open the account or commence the relationship (or **do not perform** the transaction);
- If already in relationship, **terminate**; and
- **Report an unusual transaction** where there is a **presumption of ML/TF/PF**.

4.7 Documentation & audit trail

We maintain CDD records sufficient to **reconstruct individual transactions** and to evidence decisions, for ≥ 5 years after the relationship ends (see Record-Keeping section).

Section 5 — Enhanced Due Diligence (EDD)

5.1 When EDD applies

We apply EDD whenever the **risk of ML/TF/PF is higher**, including (non-exhaustive):

- **Politically Exposed Persons (PEPs) — international and domestic**, and their **family members** and **close associates (RCAs)**;
- Exposure to **higher-risk countries**;
- Use of **new technologies** or delivery channels presenting elevated risk;
- **Other higher-risk situations** identified by the BRA/CRA or through monitoring (e.g., complex funding patterns, rapid cycling, multiple instruments).

5.2 Minimum EDD measures

In high-risk cases we will, **at a minimum**, apply one or more of the following measures, commensurate with risk:

- a) **Obtain additional information on the player**, such as occupation and relevant asset/wealth information (including reputable public databases/open-source checks).
- b) **Increase refresh frequency** of identification/verification data.
- c) **Obtain Source of Funds (SoF) and Source of Wealth (SoW)** with **independent and reliable evidence** where appropriate.
- d) **Obtain information on the reasons for intended/performed transactions** that are material or unusual relative to profile.
- e) **Senior-management approval** to commence or continue the business relationship.
- f) **Enhanced ongoing monitoring** (greater control frequency/timing; targeted patterns for review).

5.3 EDD for PEPs & RCAs (specifics)

- **Screening:** We screen for PEP status at onboarding and on risk-sensitive triggers thereafter (link to Section 4).

- **Controls:** For confirmed PEPs/RCAs we **must** (i) obtain **senior-management approval** to onboard/continue, (ii) collect **SoF/SoW** evidence commensurate with risk, and (iii) place the customer under **enhanced monitoring**.
- **De-PEP:** If a customer ceases to be a PEP, residual risk is reassessed based on **family/associate links** and current exposure; EDD may be maintained where risk remains elevated. (Rationale: PEP exposure is explicitly called out in the Curaçao framework.)

5.4 Higher-risk countries & sanctions interface

- Where a player's profile includes **higher-risk country** exposure, the CRA must reflect this with proportionate **EDD measures** (e.g., SoF/SoW evidence, payment-rail restrictions, enhanced monitoring).
- **Sanctions** screening continues per Section 4. Where a **UN/EU sanctions** hit is identified, **no relationship** is permitted and applicable **UTR objective indicators** and blocking actions apply.

5.5 New technologies & delivery channels

Before introducing higher-risk **new products/payment rails/tech**, conduct a **pre-implementation risk assessment** and document **EDD controls** (including monitoring scenarios and staff training) prior to launch.

5.6 Documentation & auditability

All EDD decisions (risk rationale, measures selected, SoF/SoW evidence, senior-management approval, monitoring settings) are **documented** and retained with CDD records in accordance with **record-keeping** requirements (**≥ 5 years** after relationship end/occasional transaction).

5.7 Inability to complete EDD

If we cannot complete required EDD measures, we **do not** commence or continue the relationship and assess for **Unusual Transaction Reporting** where a **presumption of ML/TF/PF** exists (see Section 7).

Section 6 — Simplified Due Diligence (SDD)

6.1 When SDD may apply

We may apply **simplified CDD** where the **risk of ML/TF/PF is demonstrably lower**, based on the Customer Risk Assessment (CRA) and our Business Risk Assessment (BRA). SDD is **risk-based** and must reflect the **nature of the lower risk** identified.

6.2 Prohibitions (SDD never allowed)

SDD **must not** be used:

- where there is **suspicion** of ML/TF/PF;
- in any **higher-risk scenario** (e.g., PEPs/RCAs, higher-risk countries, other factors rated “High” in the CAP/CRA);
- where sanctions screening raises a concern.

6.3 Minimum onboarding under SDD

Even when SDD applies, we **still**:

- collect **personal details** at onboarding and conduct **sanctions screening**;
- complete full CDD **no later than** reaching **NAf 4,000** (see Section 4). Players cannot deposit/withdraw beyond the threshold until standard CDD measures are completed.

6.4 Examples of SDD measures (choose proportionately)

When justified by a **low-risk** assessment, we may implement one or more of the following:

- a) **Defer full ID/BO verification until after** establishing the relationship (but always before/at NAf 4,000, or sooner if risk changes).
- b) **Reduce the frequency** of identification/verification **updates**.
- c) **Reduce the degree of ongoing monitoring/scrutiny** using a **reasonable monetary threshold** suited to the lower risk.
- d) **Do not collect specific information** on purpose/intended nature **where it is self-evident**, inferring it from the relationship/transactions (casino context).

6.5 Guardrails & dynamic review

- SDD settings are **reassessed** if player behaviour, geography, products, or channels **change risk** (e.g., unusual patterns, values just under objective

indicators). If risk increases, we **lift** SDD to standard CDD or EDD and **refresh** documentation accordingly.

- Ongoing monitoring **continues** under SDD (albeit reduced), including linkage of multiple accounts and detection of third-party identities.

6.6 Documentation & audit trail

For each account where SDD is applied, the CO/MLRO keeps **workpapers** recording: (i) the **low-risk rationale** from CRA/CAP, (ii) which **SDD measures** were used, (iii) any **thresholds** for reduced monitoring, and (iv) **review dates**. Records are retained per the Record-Keeping section (≥ 5 years).

Section 7 — Unusual Transaction Reporting (UTR) to FIU Curaçao

7.1 Purpose & definition

We identify and report **unusual transactions** (or intended transactions) to **FIU Curaçao**. An unusual transaction is a transaction or series that is **inconsistent with the player's profile** or that meets **objective indicators** set by regulation. Reports are filed by the **CO/MLRO** via **goAML**.

7.2 Objective indicators (mandatory UTR)

The CO/MLRO **must submit a UTR within 48 hours** when any **single** qualifying event occurs:

- a) ML/TF transactions reported to **police/judicial authorities**;
- b) Intended transaction by a person on a **UN or EU sanctions list**;
- c) Any **transaction $\geq$ NAf 5,000**;
- d) Any **bank transaction $\geq$ NAf 5,000**;
- e) **Sale of chips/credits $\geq$ NAf 5,000**;
- f) **Payment of prizes $\geq$ NAf 5,000**.

Objective indicators are **reported regardless of suspicion**.

7.3 Subjective indicator (risk-based UTR)

We submit a UTR when there is **reason to assume** a transaction **may be related to ML/TF** (examples below). **Internal report to the CO must be made within 24**

hours; the CO has 10 working days to research. If ML/TF is presumed, the **CO files to FIU within 48 hours** of that determination.

7.4 Examples to guide subjective assessments (non-exhaustive)

- Dozens of accounts with deposits just **below thresholds**, then rapid withdrawals.
- Regular deposits/transactions at **similar amounts**, without economic rationale.
- Funding with cards/prepaid/cheques/crypto then promptly requesting payout.
- Income/funding **inconsistent with known financial situation**.
- Claiming machine credits/payouts with no jackpot; parallel even-money betting.
- Betting against associates/intentional losses (e.g., poker/roulette) to transfer value.
- Multiple/little-purpose **currency exchanges**, or **wire transfers just under thresholds**.
- Frequent cash-outs without corresponding buy-ins; association with **multiple accounts/aliases**.

7.5 Submission channel & language

All UTRs are submitted **in English** via the **FIU Curaçao goAML portal** (registration required).

7.6 Internal escalation flow (who does what, when)

1. **Frontline/monitoring systems** detect an objective indicator **or** staff form a **subjective suspicion**.
2. Staff submit an **Internal Suspicious Activity Report (iSAR)** to the **CO** (**≤ 24 hours** for subjective cases; immediate for objective cases).
3. **CO/MLRO** reviews, gathers evidence, and:
 - **Objective: files UTR within 48 hours** of the triggering event.
 - **Subjective: completes research within 10 working days**; if ML/TF is presumed, **files within 48 hours**.

4. **Record & restrict:** apply any risk controls needed (e.g., freezes, limits) consistent with tipping-off rules.

7.7 Currency handling

Objective thresholds are measured in **Netherlands Antillean guilders (NAf)**. For non-NAf transactions, we **convert at the official rate on posting** and assess against **NAf 5,000**. (Internal SOP sets the conversion feed and timestamp.)

7.8 Confidentiality & tipping-off

All UTRs, analyses, and FIU interactions are **confidential**. Employees must **not inform** the player or third parties that an internal or external report was made (prohibition on tipping-off).

7.9 Record-keeping

We retain **internal and external UTRs** and all **supporting documents** for **≥ 5 years**, enabling transaction reconstruction and audit testing (see Record-Keeping section).

7.10 Controls & QA

- **Automation:** system rules flag any **single ≥ NAf 5,000** event type and queue a goAML draft to the CO; maintain **de-duplication** to avoid double-filing.
- **Analytics:** scenarios for **structuring just under 5k** and **rapid D/W cycling** feed subjective reviews.
- **Quality checks:** periodic sampling of iSARs, UTR timeliness (48h/10-day KPIs), and completeness.
- **Training:** targeted refreshers for high-exposure teams (Payments/Fraud, VIP, CS).

Section 8 — AML/CFT/CFP Program & Internal Controls

Our AML/CFT/CFP program comprises: (a) a **system of internal policies, procedures, and controls**; (b) a **designated Compliance Officer (CO/MLRO)**; (c) **employee screening & training**; and (d) an **independent audit function**. Policies are **Board-approved** and **communicated to employees**.

8.2 System of internal policies, procedures & controls

- **Policy stack:** this Policy; CDD/EDD/SDD Procedures; CAP/CRA; Sanctions & PEP SOP; UTR/goAML SOP; Record-Keeping Standard; Training Plan; Independent Audit Plan.
- **Procedures → practice:** operating procedures translate policy into workable steps, including thresholds, timelines (NAf 4,000 CDD; NAf 5,000 UTR objective indicators), escalation paths, and evidence requirements.
- **Internal controls (minimum):**
 - onboarding & sanctions screening gates;
 - monitoring scenarios (structuring, rapid D/W cycling, multiple instruments, under-threshold patterns);
 - automated **objective-indicator** detection (≥ **NAf 5,000** event types) with goAML draft queue;
 - account-linkage & multi-account detection;
 - exception logging & remediation tracking;
 - segregation of duties between customer-facing, payments/fraud, and CO functions.

8.3 Designated Compliance Officer (CO/MLRO)

The CO/MLRO maintains the AML program; verifies compliance with laws and internal policies; **trains employees**; manages **internal/external UTRs**; and provides **management reporting**. A formal job description is maintained.

8.4 Employee screening & training (program anchors)

We screen employees (e.g., **criminal-record checks**) and operate a risk-based **training program** with **role-specific content**, periodic **refreshers**, and **training records** retained.

8.5 Independent audit function

An **annual** internal or external **independent audit** assesses the AML/CFT program against the minimum coverage in the regulations. Reports go to the **Board**, and management's responsiveness to findings is evaluated.

8.6 Management information (MI) & Board reporting

The CO/MLRO provides periodic MI to Senior Management and the Board covering, at a minimum:

- CDD/EDD/SDD metrics (volumes, cycle-times, **NAf 4,000** threshold hits, 30-day terminations);
- UTR stats (objective vs. subjective; **48-hour** and **10-day** timeliness KPIs; FIU feedback);
- sanctions/PEP alerts & dispositions;
- training completion and testing results;
- audit actions & remediation status;
- key BRA/CRA movements and control effectiveness.

8.7 Control testing & quality assurance

Compliance performs periodic **control testing** (e.g., sample file reviews, alert calibration checks, reconciliations of objective-indicator events to UTR filings, goAML data-quality checks), documents deficiencies, assigns owners and due dates, and tracks remediation to closure (see Independent Audit interaction).

8.8 Documentation & evidence

We maintain all AML program records—including policies, procedures, CO job description, FIU registration proof, UTRs (internal/external) and support, employee-screening evidence, training plan & records, **independent audit report**, and BRA/CRA workpapers—available for GCB examination.

Section 9 — Compliance Officer (MLRO)

9.1 Appointment & independence

The Board appoints a **Compliance Officer / MLRO (CO/MLRO)** with sufficient **authority, seniority, and independence** to implement and maintain the AML/CFT/CFP program. A **deputy** is designated to act in the CO's absence. A formal **job description** is maintained and available for inspection.

9.2 Responsibilities

The CO/MLRO is responsible for:

- Maintaining the **AML/CFT/CFP program** and associated policies, procedures, and internal controls.
- **Verifying compliance** with applicable laws, regulations, and internal policies.
- Designing and delivering **training** (role-based, refreshers) and keeping **training records**.
- Receiving internal suspicious activity reports (iSARs) and submitting **UTRs to FIU Curaçao via goAML** within the required timelines (objective ≤ 48h; subjective: internal ≤ 24h, research ≤ 10 working days, then ≤ 48h to file if presumed ML/TF).
- Providing **management information (MI)** and **reports** to Senior Management and the **Board** (e.g., CDD/EDD/SDD metrics, UTR KPIs, sanctions/PEP alerts, training status, audit actions, BRA/CRA movements).
- Maintaining evidence required for **GCB examination** (policy register, FIU registration proof, UTR files, screening and training records, audit reports, job description, management reports).

9.3 Reporting line & access

The CO/MLRO reports to the **Board** (or a Board committee) with **unrestricted access** to management and records necessary to discharge duties. Periodic written reports are tabled to the Board and minuted.

9.4 Resources & escalation rights

The CO/MLRO must have adequate **resources, systems, and staffing** to operate the program, and explicit authority to **escalate and enforce** risk mitigations (e.g., account restrictions/closure, enhanced monitoring) consistent with law and internal policy.

9.5 Conflicts & confidentiality

Potential **conflicts of interest** affecting the CO's independence are disclosed to, and managed by, the Board. All iSARs/UTRs and related analyses are **confidential**; **tipping-off is prohibited**.

Section 10 — Employee Screening & Training

10.1 Objectives

Ensure all relevant staff are fit and proper to perform AML-sensitive roles and are trained to identify, escalate, and help prevent ML/TF/PF, in line with Curaçao's AML program requirements.

10.2 Employee screening (pre-employment & ongoing)

- **Pre-employment checks (risk-based):** identity, right-to-work, **criminal-record check**, CV verification, references; additional checks for AML-critical roles (e.g., CO/MLRO, Payments/Fraud, VIP).
- **Independence/conflicts:** declare and manage conflicts (e.g., personal relationships with players or third parties).
- **Ongoing screening:** repeat/refresh checks proportionate to role risk and on role change or adverse information (document rationale and outcomes).
- **Records:** maintain screening **program** and **screening records** for GCB examination.

10.3 Training program (design & governance)

- **Program design:** documented **training plan** covering AML/CFT/CFP concepts, local thresholds and timelines (**NAf 4,000 CDD**, **NAf 5,000 objective UTR**, internal $\leq 24\text{h}/10\text{-day}/48\text{h}$ rules), sanctions/PEP screening, iSAR → UTR flow, tipping-off prohibition, and record-keeping (≥ 5 years).
- **Role-specific content:** different training for **different employees** (e.g., Payments/Fraud, VIP/CS, RG, Tech/BI, CO/MLRO).
- **Refresh cadence:** **initial onboarding** plus **periodic refreshers**; frequency set by risk (at least annually for high-exposure teams).
- **Assessment & attestations:** knowledge checks and annual attestations of understanding; failed assessments trigger remedial training.
- **Delivery & access:** training is tracked centrally; materials are accessible to employees and available to regulators on request.
- **Records:** keep **training plan** and **training records** (attendance, results, content versions).

10.4 Minimum training syllabus (by audience)

- **All staff:** AML/CFT/CFP basics; recognizing red flags; **how to file an internal report**; confidentiality/**tipping-off prohibition**; who the CO/MLRO is and how to reach them.
- **Customer-facing & Payments/Fraud/VIP/CS:** scenarios from gaming typologies (structuring just under thresholds, rapid deposit/withdrawal cycling, parallel even-money betting, intentional losses, multiple instruments), sanctions/PEP alerts handling, iSAR quality standards.
- **CO/MLRO & Compliance:** goAML submission standards, data quality, timeliness KPIs, management reporting, audit preparation.
- **Tech/Data/BI:** monitoring rules, alert calibration, objective-indicator capture ($\geq$ **NAf 5,000** event types), data retention & reconstructability.

10.5 Quality assurance

Compliance periodically samples training records and **screens completed iSARs/UTRs** for linkage to training topics; gaps drive targeted refreshers. (Part of the AML program's internal controls and audit readiness.)

Section 11 — Independent Audit of the AML Program

11.1 Purpose

Provide an objective assessment of whether the AML/CFT/CFP program is designed and operating effectively and in line with Curaçao's requirements.

11.2 Frequency & independence

An **independent audit** of the AML/CFT program is performed **annually** by internal audit or a qualified external party that is operationally independent from Compliance and first-line functions.

11.3 Minimum coverage

The audit, at a minimum, evaluates:

- **Policies, procedures, and internal controls** (design & operating effectiveness; Board approval; communication to employees).
- **Risk-based approach artifacts:** BRA methodology, approvals, updates; CAP/CRA operation.

- **CDD/EDD/SDD** (including NAF 4,000 timing/blocks; PEP handling; higher-risk countries; new technologies).
- **Sanctions & PEP screening** controls and dispositions.
- **Unusual Transaction Reporting (UTR)**: objective/subjective indicators, **48-hour** and **10-working-day** timelines, goAML data quality.
- **Employee screening & training** program and records.
- **Record-keeping** (≥ 5 years, reconstructability).
- **CO/MLRO governance**: role, authority, reporting lines, MI to management/Board.

11.4 Reporting & remediation

- The auditor issues a **written report to the Board**, including findings, ratings, and recommendations.
- Management prepares and executes a **remediation plan**; the audit assesses **responsiveness to findings** in subsequent cycles.

11.5 Workpapers & evidence retention

Audit workpapers, sampling frames, test results, and management responses are retained with the AML program evidence set and made available for GCB examination (see Section 8.8).

11.6 Interaction with Compliance monitoring

This audit is **independent of** ongoing Compliance QA/testing (Section 8.7) and relies on risk-based sampling rather than solely on the first/second-line monitoring outcomes.

Section 12 — Record Keeping & Data Management

12.1 Objectives & minimum standard

We maintain records sufficient to (a) **reconstruct individual transactions** and (b) evidence our AML/CFT/CFR controls and decisions, for the periods required under Curaçao's framework.

12.2 Retention periods

- **Transaction records:** keep **all necessary records** for **≥ 5 years**.
- **CDD/EDD/SDD records:** keep for **≥ 5 years after the business relationship ends** or after an **occasional transaction**.

Note: These are minimum periods; longer retention may apply where legally required (e.g., litigation hold, regulator instruction).

12.3 Records we retain (minimum set)

- **Player identification** & verification artifacts (ID images/data, address proofs, sanctions/PEP screening hits & dispositions).
- **Customer Risk Assessment (CRA), risk profile (L/M/H),** and changes over time.
- **Business relationship activity:** deposits, withdrawals, transfers, payment-instrument metadata, session/account linkage evidence (multi-account detection).
- **Analyses & communications:** investigator notes, internal emails/chats with players, outcome of reviews (SoF/SoW, EDD rationales).
- **Unusual Transaction Reports (UTRs):** internal iSARs, external goAML filings, supporting documentation, FIU correspondence.
- **Program evidence for examination:** BRA & sources, CAP/CRA, policy/procedure versions, CO/MLRO job description, FIU registration proof, training plan & **training records**, employee screening records, independent audit report, management reports to Board.

12.4 Transaction reconstructability

Records must allow reconstruction of **who, what, when, amount, instrument, currency, counterparties, and outcomes** for each transaction, including:

- **Time-stamped ledgers** and payment rails used;
- **FX/NAf conversion evidence** used to assess **NAf 4,000 CDD** and **NAf 5,000** objective UTR thresholds; retain the **rate source** and timestamp applied at posting.

12.5 Data quality, integrity & access

- **Integrity:** maintain versioning/immutability for key AML artifacts (CRA, EDD decisions, UTR packs); preserve original files and audit trails.
- **Availability:** records must be **readily retrievable** to respond to GCB/FIU requests within required timeframes.
- **Confidentiality:** apply least-privilege access; protect UTR/iSAR confidentiality (tipping-off prohibition).

12.6 Storage & security

Store records in secure systems with access controls, encryption at rest/in transit (where applicable), and monitored backups. Identify and tag regulated AML records to ensure they are not deleted before the minimum retention period.

12.7 Disposal

At the end of the retention period (unless a legal hold applies), dispose of records **securely** and in a way that prevents reconstruction (document method/date and authorizer).

12.8 Outsourcing & third parties

Where any AML function (e.g., screening, KYC) is outsourced, ensure **we can obtain all underlying records** without delay and that third-party contracts embed equivalent retention, security, and access requirements (ultimate responsibility remains with us).

Section 13 — High-Risk Countries & Sanctions / CFP Controls

13.1 Objectives

Prevent relationships/transactions involving sanctioned persons/entities and manage **higher-risk country** exposure, including **proliferation-financing (PF)** risk, in line with FATF **R19** and Curaçao's AML/CFT/CFP framework.

13.2 Sanctions screening (scope & sources)

- We screen all players **at onboarding** and **on a risk-sensitive basis** thereafter against at least:
 - **EU sanctions** (EU sanctions map), and **US OFAC SDN** lists.

- Screening also runs on **trigger events** (e.g., PEP status change, country move, payment-instrument change, adverse media).
- **Hits** are reviewed, documented (true/false positive), and dispositions recorded. Where a **true hit** is confirmed, **no relationship** is permitted (or it is **immediately terminated**), account is blocked, and required reports are filed (see 13.5/Section 7).

13.3 High-risk countries (risk treatment)

- Country risk is assessed in the **CRA/CAP** and **BRA**. Exposure to **higher-risk countries** requires **EDD** proportional to risk (e.g., SoF/SoW with independent evidence, first-payment rule, tighter limits, enhanced monitoring) or **decline** if outside risk appetite.
- Country-risk inputs include FATF statements and other credible sources; outcomes are reflected in the player's **risk rating** and controls.

13.4 PF (Counter-Proliferation Financing) controls

- Sanctions screening and higher-risk-country controls apply equally to **PF** exposure.
- Any PF-relevant matches (e.g., UN/EU-listed persons/entities) lead to **immediate blocking** and escalation to the **CO/MLRO** for external reporting per Section 7.

13.5 Objective UTR link (sanctions & police reports)

The **CO/MLRO** must submit a UTR within 48 hours for any of the **objective indicators**, including:

- **Intended transaction by a person on a UN or EU sanctions list;**
 - **ML/TF transactions reported to police/judicial authorities.**
- (These are reported **regardless of suspicion** via **goAML**, in **English**.)

13.6 Operating standards (minimum)

- **List currency & frequency:** keep sanctions sources current; document update cadence and the version consulted at match time.
- **Name-matching quality:** use tools capable of fuzzy/alias matching; record match strength and rationale for clear false positives.

- **Blocks & exceptions:** on positive matches, **block immediately**, freeze pending movements, and follow Section 7 timelines; any temporary exception requires **CO/MLRO written approval** and Board notification per Section 1.8.
- **MI/QA:** include sanctions/high-risk-country metrics and dispositions in periodic MI to management/Board (see Section 8.6).

13.7 Documentation & retention

Maintain auditable records of screening events, list versions, match analysis, decisions, and any UTRs filed for **≥ 5 years** (see Section 12).

Section 14 — New Technologies & Delivery Channels

14.1 Objective

Identify, assess, and mitigate ML/TF/PF risks arising from **new products, payment rails, delivery channels, or technologies** (per FATF **R15**) before launch, and calibrate controls proportionately thereafter.

14.2 Pre-implementation risk assessment (mandatory before go-live)

Before introducing any new/changed technology or channel (e.g., new PSPs, wallets, faster payouts, biometric onboarding, automated KYC vendors, in-app features), the CO/MLRO ensures a written assessment that:

- Describes the **use case**, actors, data flows, and jurisdictions involved.
- Evaluates **player, country, product, service, and delivery-channel** risk factors and relevant NRA items.
- Maps risks to **controls** (CDD/EDD/SDD implications, sanctions/PEP screening touchpoints, monitoring scenarios, UTR triggers, record-keeping).
- Sets **go/no-go conditions**, success metrics, and post-launch review dates.
- Documents **Board approval** where risk is material (aligns with BRA governance).

14.3 Minimum controls for new tech/channels

At launch (and ongoing), we will at least:

- a) **CDD timing gates:** enforce **NAf 4,000** timing/blocks and the **30-day** termination rule in the new flow.
- b) **Objective-indicator capture:** ensure single-event $\geq$ **NAf 5,000** triggers (txn, bank txn, sale of credits, prize) feed the **goAML** queue within **48h**.
- c) **Scenario monitoring:** calibrate alerts for structuring just under thresholds, rapid deposit/withdrawal cycling, multiple instruments, account linkage/third-party identities.
- d) **Sanctions/PEP touchpoints:** screening at onboarding and risk-sensitive intervals within the new channel.
- e) **Record-keeping:** ensure $\geq$ **5 years** retention and **transaction reconstructability** (who/what/when/amount/instrument/FX to NAf).
- f) **Training:** targeted enablement for impacted teams before go-live; update procedures and playbooks.

14.4 Post-implementation review & model tuning

Within **60–90 days** post-launch (or sooner on adverse signals), Compliance reviews: alert precision, UTR timeliness (48h/10-day KPIs), false-positive rates, and any control gaps, then retunes thresholds and documents changes for audit.

14.5 Elevated-risk use cases (EDD overlay)

For features deemed **higher risk** in the assessment (e.g., novel payment instruments, cross-border payout corridors, accelerated withdrawals), apply **EDD** such as: **senior-management approval**, first-payment from an account in the player's name at a CDD-standard bank, and stronger SoF/SoW evidence and monitoring until residual risk is acceptable.

14.6 Change management & kill-switch

- Material control changes (rules, thresholds, vendor switches) follow documented **change control** with CO sign-off and rollback plan.
- A **kill-switch** (ability to suspend the new feature/channel) must exist if risk exceeds appetite or critical control fails (e.g., sanctions screening outage), with incident logged and Board notified via MI cycle.

14.7 Documentation

Maintain the risk assessment, approvals, go-live checklist, monitoring calibration notes, training evidence, and post-implementation review in the AML program evidence set for GCB examination.

Section 15 — Reliance on Third Parties & Outsourcing

15.1 Purpose & principle

We may outsource certain AML activities (e.g., sanctions/PEP screening, ID&V) or **rely on third parties** for elements of CDD **only where risk-appropriate**.

Reliance/outsourcing **does not transfer responsibility**: Slotbox N.V. remains fully accountable for compliance and reporting.

15.2 Due diligence on providers (before onboarding)

- **Competence & coverage**: technical capability for our markets, lists, and document sets; uptime/latency suitable for onboarding flows.
- **Regulatory fit**: ability to meet Curaçao thresholds/timelines (**NAf 4,000** CDD timing; objective **NAf 5,000** capture for UTR analytics inputs).
- **Data, security & privacy**: evidence of secure storage, access controls, retention $\geq$ **5 years**, and export on demand for **transaction reconstruction** and examinations.
- **Auditability**: independent audits/certifications; acceptance of our audit and regulator access rights.

15.3 Mandatory contract terms (minimum)

Contracts (MSA/SOW/DPA) must include:

- a) **Scope** of services and **controls** provided (screening lists, match logic, thresholds).
- b) **Service levels** (hit-rate KPIs, turnaround times, uptime), **quality** and **false-positive** management.
- c) **Right to obtain all underlying records promptly**, without charge beyond agreed fees; **format** and **timelines** defined.
- d) **Right to audit/inspect**, including by the GCB/FIU upon request; cooperation with investigations.

- e) **Sub-processor controls** (approval, flow-down obligations).
- f) **Incident & change management:** notifications, rollback/kill-switch; material changes pre-approved by CO/MLRO (aligns with Section 14).
- g) **Termination/transition assistance** and **data return**/destruction obligations meeting retention rules (**≥ 5 years**).

15.4 Operating standards & oversight

- **Owner:** CO/MLRO oversees all AML-relevant providers and maintains a register (scope, KPIs, last review date, audit status).
- **Initial & periodic testing:** file sampling (ID quality, address proofs, sanctions match handling), latency/uptime checks, and reconciliation of **objective-indicator events** (**≥ NAf 5,000**) into our UTR pipeline.
- **Performance MI:** provider KPIs (match quality, turnaround, outages) included in Compliance MI to Senior Management/Board (Section 8.6).
- **Records:** retain vendor DD pack, contracts, service evidence, results of testing, and any corrective actions for **GCB examination**.

15.5 Player communication & transparency

Where third-party tools are used in onboarding/screening, disclosures in T&Cs/privacy notices must cover information sharing and verification methods (without compromising tipping-off restrictions).

15.6 Failure or inability of third party

If a third party **cannot** complete required CDD elements or **fails**, we **do not** commence/continue the relationship and assess for UTR where a presumption of ML/TF/PF exists (see **Sections 4 & 7**).

Section 16 — Quality Assurance & Management Information (MI)

16.1 Objective

Provide ongoing evidence that AML/CFT/CFP controls are designed well, operating effectively, and improving over time; give Senior Management and the Board clear visibility of risk, performance, and issues.

16.2 QA scope (what we test)

- **Onboarding & CDD timing gates:** NAf 4,000 threshold logic, 30-day termination rule, sanctions/PEP checks run and documented.
- **EDD execution:** presence/quality of SoF/SoW evidence, senior-management approvals, enhanced monitoring set correctly.
- **UTR workflow:** objective-indicator capture (single $\geq$ NAf 5,000 events) and subjective case handling; internal ≤ 24 h intake, research ≤ 10 working days, external filing ≤ 48 h.
- **Monitoring scenarios:** calibration of alerts (structuring under thresholds, rapid D/W cycling, multiple instruments, multi-accounting/third-party use).
- **Record-keeping:** reconstructability of transactions and completeness of CDD/UTR packs (≥ 5 years).
- **Training & screening:** staff in scope completed training; key roles screened appropriately.
- **Third parties:** KYC/screening vendors meeting SLAs; data exportability, audit rights, outage handling.

16.3 QA methods (how we test)

- **File sampling:** risk-based monthly samples across Low/Med/High risk; targeted "deep dives" on outliers.
- **Control walkthroughs:** end-to-end tests from alert to disposition and, where relevant, to UTR.
- **Data checks:** reconcile objective events ($\geq$ NAf 5,000) vs. UTR filings; currency conversion logic to NAf; de-duplication controls.
- **Model/rule tuning reviews:** precision/recall checks; false-positive/false-negative analysis with documented adjustments.
- **Issue management:** log findings with owners, severities, deadlines; track remediation to closure.

16.4 Governance & cadence

- **Owner:** CO/MLRO.
- **Cadence:** QA testing monthly; MI monthly to SMT and quarterly to Board; ad-hoc on material incidents.

- **Change control:** material rule/threshold changes recorded (rationale, owner, date), with kill-switch readiness where applicable.
- **Escalation:** red-rated issues and overdue remediations escalated to SMT and tabled to the Board.

16.6 Documentation & evidence

Maintain QA plans, sampling frames, test scripts, results, issues logs, remediation evidence, and MI packs for regulator examination and audit.

Section 17 — Breaches, Incident Handling & Disciplinary Measures (incl. tipping-off prohibition)

17.1 Objectives

Detect, log, investigate, remediate, and report AML/CFT/CFP control breaches and incidents in a way that protects players, the business, and the integrity of investigations—without tipping off any subject.

17.2 Definitions

- **Breach:** Failure to comply with a law, regulation, licence condition, or this Policy/procedures (e.g., missed CDD timing, late UTR).
- **Incident:** An event that degrades control effectiveness (e.g., sanctions-screening outage, monitoring rule misfire), even if no breach has yet occurred.
- **Tipping-off:** Any disclosure to a player/third party that an internal investigation or UTR/SAR has been or may be filed.

17.3 Severity levels (for triage & escalation)

- **Sev 1 — Critical:** Actual/likely regulatory breach with customer or FIU impact (e.g., objective-indicator UTR not filed within 48h; sanctions true-hit not blocked).
- **Sev 2 — Major:** Material control failure with heightened risk but no confirmed breach (e.g., CDD block misconfigured for a cohort, delayed research beyond 10 working days).
- **Sev 3 — Moderate:** Localised process lapse or training gap; limited risk.
- **Sev 4 — Minor:** Cosmetic/documentation issues; no risk change.

17.4 Detection & intake (who can raise, how fast)

- **Anyone** (staff, systems, vendors) must raise suspected breaches/incidents **immediately** via the compliance ticket queue or email to the **CO/MLRO**.
- Objective-indicator events detected by systems ($\geq$ **NAf 5,000** single events; sanctions true hits) are **auto-queued** to Compliance for filing/blocks.

17.5 Investigation workflow (time-bound)

1. **Log & acknowledge** (owner = CO/MLRO). Assign **severity** and case owner; record timestamp and facts.
2. **Stabilise risk**: apply interim controls (e.g., limits, holds, temporary blocks) consistent with the tipping-off prohibition.
3. **Root-cause analysis (RCA)**: identify control, process, system, data, or training causes; capture evidence.
4. **Regulatory handling**:
 - **Objective UTR**: file within **48 hours** of the triggering event.
 - **Subjective case**: intake within **24 hours**, research within **10 working days**; if ML/TF is presumed, file within **48 hours** of that determination.
5. **Remediation plan**: actions, owners, due dates, required policy/procedure/config changes.
6. **Closure & QA**: verify fix in production; update run-books; note lessons learned.

17.6 Escalation & reporting

- **Sev 1/2**: immediate notification to Senior Management; tabled to the **Board** at the next cycle (or sooner if material).
- External regulator/FIU engagement is coordinated by the **CO/MLRO**; all correspondence is archived with the case file.

17.7 Disciplinary measures & accountability

- Intentional misconduct, gross negligence, or repeated non-compliance may result in disciplinary action up to and including termination, consistent with HR policy and local law.

- Managers are accountable for ensuring teams follow procedures, complete training, and remediate findings on time.

17.8 Whistleblowing & non-retaliation

Good-faith reports of suspected breaches or ML/TF are encouraged. Retaliation against reporters is prohibited and will itself be treated as a serious breach.

17.9 Tipping-off prohibition (operational guardrails)

- Do **not** inform a player/third party that an internal iSAR or external UTR/SAR is being considered or filed.
- Communications with players during reviews use **neutral wording** (e.g., “standard compliance checks”).
- Access to UTR/iSAR content is **restricted** on a need-to-know basis.
- All external enquiries relating to AML investigations are routed to the **CO/MLRO**.

17.10 Documentation & retention

Maintain a complete case record (facts, timestamps, evidence, RCA, decisions, filings, correspondence, remediation, and verification) for **≥ 5 years** with cross-references to any related UTRs, CDD files, and policy changes.

17.11 Metrics & continuous improvement

Include in the MI pack (Section 16): count by severity; time-to-detect/contain/close; UTR timeliness (24h/10-day/48h); recurring causes; overdue remediations; control re-tests post-fix. Use trends to prioritise audits, training, and rule tuning.

Section 18 — Appendices

Appendix A — Definitions & Abbreviations

- **AML/CFT/CFP**: Anti-Money Laundering / Counter-Terrorist Financing / Counter-Proliferation Financing
- **BRA / CAP / CRA**: Business Risk Assessment / Customer Acceptance Policy / Customer Risk Assessment

- **CDD / SDD / EDD:** Customer Due Diligence / Simplified Due Diligence / Enhanced Due Diligence
- **CO/MLRO:** Compliance Officer / Money Laundering Reporting Officer
- **FIU / UTR (SAR):** Financial Intelligence Unit / Unusual Transaction Report (Suspicious Activity Report)
- **PEP / RCA:** Politically Exposed Person / Relative or Close Associate
- **SoF / SoW:** Source of Funds / Source of Wealth
- **NAf 4,000 / NAf 5,000:** CDD timing trigger / Objective UTR single-event trigger

Appendix B — Internal iSAR (Unusual Activity) Form (one-page)

- **Reporter:** name/role/contact | **Date/time:**
- **Player IDs/accounts involved:**
- **Description of activity:** facts, dates, amounts, instruments, screenshots/attachments
- **Why unusual:** objective/subjective indicators tick-box
- **Immediate risk controls applied:** holds/limits/blocks (no tipping-off)
- **Submitted to CO on:** (≤ 24 h for subjective; immediate if objective)

Appendix C — Training Plan & Record Log

Plan: audiences, modules, cadence, assessment method

Record fields: employee, role/team, course version, completion date, score, remedial actions, attestation received (Y/N)

Appendix D — CO contact

Email: risk@slotbox.com

Phone Number: +353862164979

Appendix E - Sanction Lists

Sanctions screening is conducted against the following sanctions lists:

- **European Union (EU) Sanctions:** The EU's Consolidated List of Sanctions (<https://www.sanctionsmap.eu>)
- **United Kingdom (UK) Sanctions:** UK Sanctions List maintained by the Office of Financial Sanctions Implementation (OFSI) (<https://www.gov.uk/government/publications/the-uk-sanctions-list>)
- **Australian Sanctions:** The Consolidated List maintained by the Department of Foreign Affairs and Trade (DFAT) (<https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>)
- **United Nations (UN) Sanctions:** The UN Consolidated List (<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>)
- **Office of Foreign Assets Control (OFAC) Sanctions:** The Specially Designated Nationals and Blocked Persons List (SDN List) and other OFAC sanctions lists (<https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>)

Appendix F – Lines of Defence

The Slotbox risk framework is based upon the Three Lines of Defence model to allow for structured roles, responsibilities and accountabilities to be built into risk decision making. The first line is business operations, with responsibility for ensuring a risk and control environment is established as part of day-to-day operations. The second line is oversight functions (e.g. MLRO), with responsibility for setting company boundaries by drafting and Implementing policies and procedures within risk appetites. The third line is independent assurance providers such as Internal & external Audit, who provide objective assurance activities designed to improve the company's operations.

