Shufti

Malta

GUIDE

Malta iGaming KYC & AML Readiness Guide

A Post-Stanleybet Control Framework for MGA-licensed Operators

VÉRIFICATION D'ÂGE KJM

PCI DSS

iBeta Niveau 1

ISO 27001: 2013

CE+

QG GDPR

SOC2

GDPR

CCPA

Executive Summary

Malta's iGaming sector operates under one of Europe's most demanding dual-regulator compliance frameworks. MGA-licensed operators must satisfy both the Malta Gaming Authority on gaming conduct and the Financial Intelligence Analysis Unit on AML/CFT controls. Both regulators hold separate enforcement powers and can act simultaneously against the same operator.

The difficulty is not knowing the obligations. Most compliance teams understand that customer identity verification, CDD, PEP screening, and transaction monitoring are required.

The challenge is not the existence of those controls. It is the data architecture behind them: do the systems link customer activity across products, brands, and outlets in a way an examiner can verify? The Stanleybet enforcement signal in March 2026 confirmed this is now an active FIAU examination priority.

This guide covers the full Malta iGaming compliance stack, including the Stanleybet failure matrix, the €2,000 CDD threshold and how to track it, the distinction between CDD and EDD, fraud threats that undermine identity controls, Markers of Harm obligations, STR workflows, FIAU evidence preparation, vendor evaluation criteria, and a 30/60/90-day implementation blueprint.

It is written for compliance officers, MLROs, fraud managers, risk teams, and product leaders at MGA-licensed B2C operators. Operators that build KYC and AML as connected infrastructure, not as separate checks added after growth begins, will be better positioned when examination scrutiny increases.

Table of Contents

What Changed After Stanleybet

On 23 March 2026, the Financial Intelligence Analysis Unit (FIAU) imposed an administrative penalty of €225,730 on Stanleybet Malta Limited, plus a periodic penalty of €2,000 per day until remediation. The penalty followed the FIAU's finding that the operator failed to identify customers, conduct Customer Due Diligence (CDD), carry out customer risk assessments, monitor customer relationships, and maintain the ability to link cumulative transactions across its retail betting network.

Stanleybet has filed an appeal, and the decision remains subject to that process. Regardless of appeal outcome, the FIAU's enforcement position is clear: for MGA-licensed operators, KYC is no longer a document check at onboarding. It is an architecture question.

The case surfaces a compliance blind spot shared by many operators: systems that track deposits per outlet or per transaction rather than per customer across every product, brand, and channel. An operator whose platform stores casino, sportsbook, and retail data in separate databases faces the same structural vulnerability that the FIAU examination identified in Stanleybet's network.

MGA-licensed operators should be able to evidence who the customer is, when the €2,000 CDD threshold was reached across relevant products, brands, channels, and outlets, which controls were triggered, what documentation was collected, and how suspicious activity was escalated to the MLRO and the FIAU.

This guide gives compliance officers, MLROs, fraud managers, risk teams, and product leaders a practical control framework covering Malta iGaming KYC, CDD triggering and evidencing, PEP and sanctions screening, fraud prevention, Markers of Harm monitoring, and FIAU examination readiness. After reading it, operators will be able to benchmark their current control architecture against the obligations an FIAU examination will assess.

[1] 2025 Digital Banking Performance Metrics." Accessed: Dec. 19, 2025. [Online].
Available: https://www.crnrstone.com/gritty-insights/research/2025-digital-banking-performance-metrics

€225,730+

€2,000/day

FIAU administrative penalty on Stanleybet Malta Limited, March 2026. Grounds: customer identification failures, CDD failures, customer risk assessment failures, monitoring failures, and inability to link cumulative transactions across outlets. Subject to operator appeal.

Source: *FIAU Publication Notice, March 2026.*

How Malta's Compliance Framework Works

Malta's iGaming compliance framework operates through two regulators with overlapping but distinct mandates. Misunderstanding where one's authority ends and the other's begins is among the most common compliance planning errors operators make.

The Malta Gaming Authority

The Malta Gaming Authority (MGA), consolidated under its current structure in 2018, holds the primary licensing and supervision mandate for all gaming activity in Malta. Under the Gaming Act (Chapter 583 of the Laws of Malta), which came into force in August 2018, the MGA issues licences, conducts compliance audits, and enforces gaming regulations.[1] The maximum administrative penalty is €500,000 per infringement, with additional powers including licence suspension and cancellation.

In 2024, the MGA initiated 43 AML/CFT compliance examinations, concluded 60 examinations, and imposed remediation measures and administrative penalties on a number of licensees.[2] The authority reported 35 warnings and €306,250 in administrative penalties in the same period.

The Financial Intelligence Analysis Unit

The Financial Intelligence Analysis Unit (FIAU) supervises all AML/CFT obligations for Malta entities, including gaming operators. Established 1 October 2002, the FIAU receives Suspicious Transaction Reports (STRs), registers MLROs, conducts AML/CFT examinations, and issues administrative fines. In 2024, the FIAU issued €504,730 in administrative fines across all sectors, with the gaming sector accounting for the largest portion.[3]

The FIAU operates under the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR, Subsidiary Legislation 373.01), which transposed the EU Fourth and Fifth Anti-Money Laundering Directives into Maltese law.[4] The FIAU's Implementing Procedures Part II for the Remote Gaming Sector (published July 2020) provides the operational guidance operators must follow for CDD, EDD, transaction monitoring, and STR workflows.[5]

[1] Gaming Act, Chapter 583 of the Laws of Malta. August 2018. legislation.mt
[2] MGA Annual Report 2024. Malta Gaming Authority. mga.org.mt/publications
[3] FIAU Annual Report 2024. Financial Intelligence Analysis Unit. fiau.org.mt/publications
[4] Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR), Subsidiary Legislation 373.01. legislation.mt
[5] FIAU Implementing Procedures Part II for the Remote Gaming Sector. September 2020provideson . fiau.org.mt

Dual-Regulator Enforcement Model

Area	MGA	FIAU
Primary mandate	Licensing & gaming compliance	AML/CFT supervision & STR receipt
Enforcement power	Fines up to €500,000, suspension	Administrative fines, AML/CFT exams
Governing legislation	Gaming Act Chapter 583	PMLFTR S.L. 373.01
2024 activity	43 exams initiated, 60 concluded	€504,730 in fines issued

The MGA requests AML/CFT examinations from the FIAU. When the FIAU finds violations, it issues fines directly to the operator. A single KYC or AML failure can trigger enforcement action by both regulators.

Regulatory Updates

The MGA published amendments to its Player Protection Directive in January 2023, with implementation obligations taking effect under the Directive's transitional provisions. The amendments introduced mandatory "Markers of Harm" monitoring requirements for all B2C licensees.

The EU Anti-Money Laundering Regulation (AMLR, Regulation 2024/1624) applies directly to gaming operators from 10 July 2027.[6] Unlike previous directives, the AMLR applies without national transposition. Gaming operators offering cross-border services fall within scope. Malta's AML/CFT credibility was strengthened after the country was removed from FATF's enhanced monitoring list in June 2022.[7]

PMLFT Function Holder Requirement

Under MGA Directive 3 of 2020, every licensed operator must designate at least one PMLFT Function Holder responsible for Prevention of Money Laundering and Financing of Terrorism.[8] The MLRO must be registered with the FIAU and must meet qualification standards: a related bachelor's degree with two years' MLRO experience, or four years as MLRO without the degree. Ten hours of continuing professional development annually are mandatory.

[6] EU Anti-Money Laundering Regulation 2024/1624 (AMLR). European Parliament and Council. eur-lex.europa.eu
[7] FATF press release: Malta removed from increased monitoring list. June 2022. Financial Action Task Force. fatf-gafi.org
[8] MGA Directive 3 of 2020. Malta Gaming Authority. mga.org.mt

2 regulators MGA and FIAU, both can audit, both can fine

A clean licensing record with MGA does not protect against a separate FIAU AML finding.

The Stanleybet Failure Matrix

The FIAU's findings against Stanleybet describe five control failures, each traceable to a specific architectural or process gap.[9] The matrix below maps each failure to its regulatory exposure, the control required to address it, and the evidence an operator must be able to produce for an FIAU examination.

Failure Mode	MGA	FIAU	FIAU
Deposits are not linked across outlets	CDD threshold missed, PMLFTR breach	Customer-level transaction spine across all outlets and products	Customer deposit ledger: cumulative 180-day total per customer
Customer not known at the control point	CDD/CRA failure, PMLFTR breac	Identity verification at onboarding, verified before threshold	Verification timestamp, document check result, liveness result
No customer risk assessment	CRA failure under FIAU Procedures Part II	Risk scoring at CDD trigger: geography, game type, velocity, VIP	Risk tier assignment, scoring criteria, and date of assessment
Monitoring not possible (no customer list)	Ongoing monitoring failure, PMLFTR breach	Unified customer identity graph across all products	Monitoring log per customer, alert history, and risk-score changes
Inadequate STR workflow	STR deadline breach	MLRO escalation workflow with same-day filing capability	Internal report, MLRO decision log, goAML filing timestamp

Why This Matters for Online Operators

Stanleybet operated retail betting shops. That enforcement position applies with equal force to online operators who store casino, sportsbook, and live gaming data in separate product databases without a unified customer identity layer. For online operators, retail formats are irrelevant. The question is: can the operator produce a single ledger showing every deposit a given customer made, across every product and channel, over the preceding 180 days?

If the answer is no, the structural gap is the same as Stanleybet's.

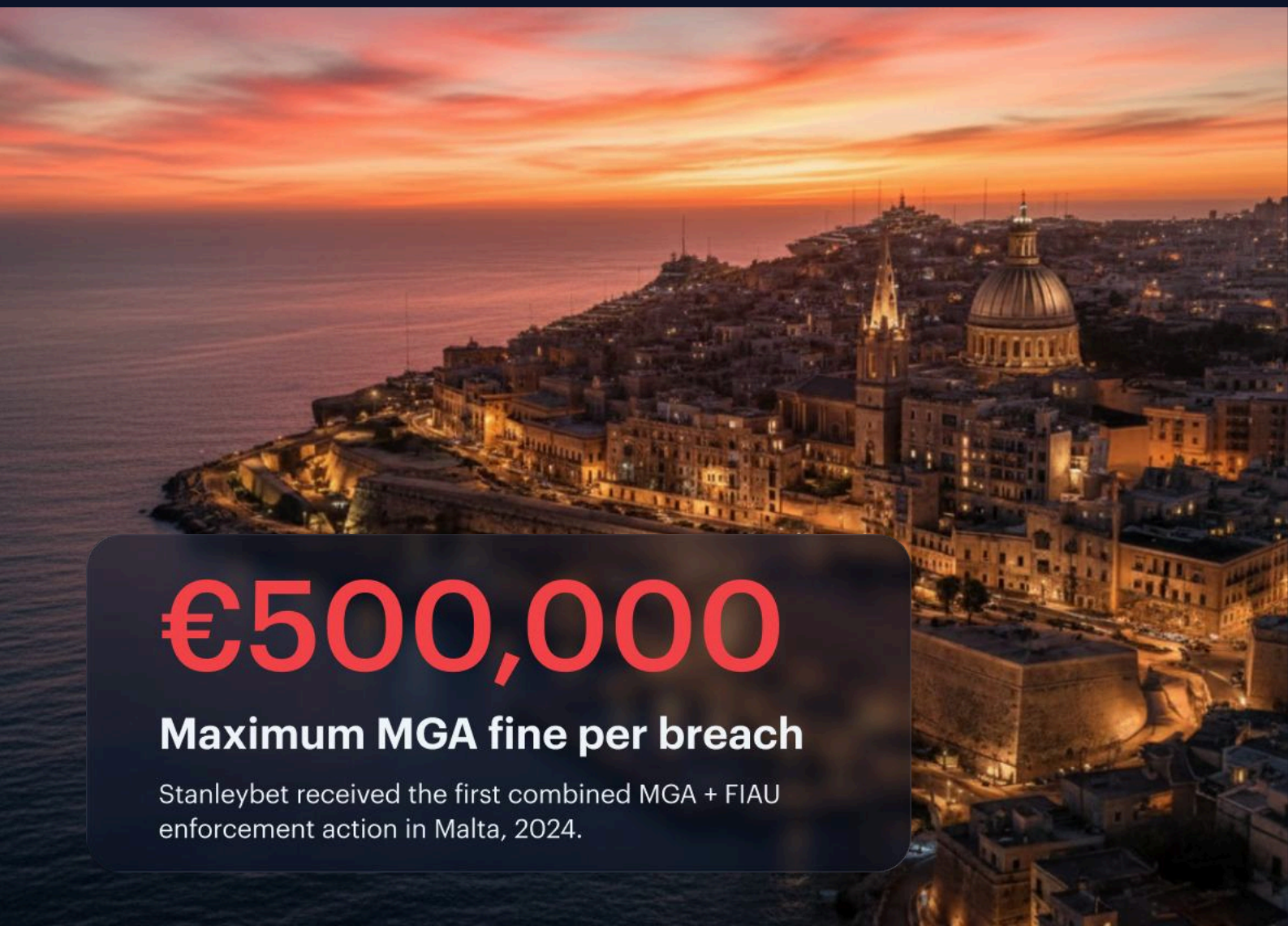
[9] FIAU Administrative Penalty Notice, Stanleybet Malta Limited. 23 March 2026. Financial Intelligence Analysis Unit. fiau.org.mt/publications

Shufti

Retail vs Online Equivalence

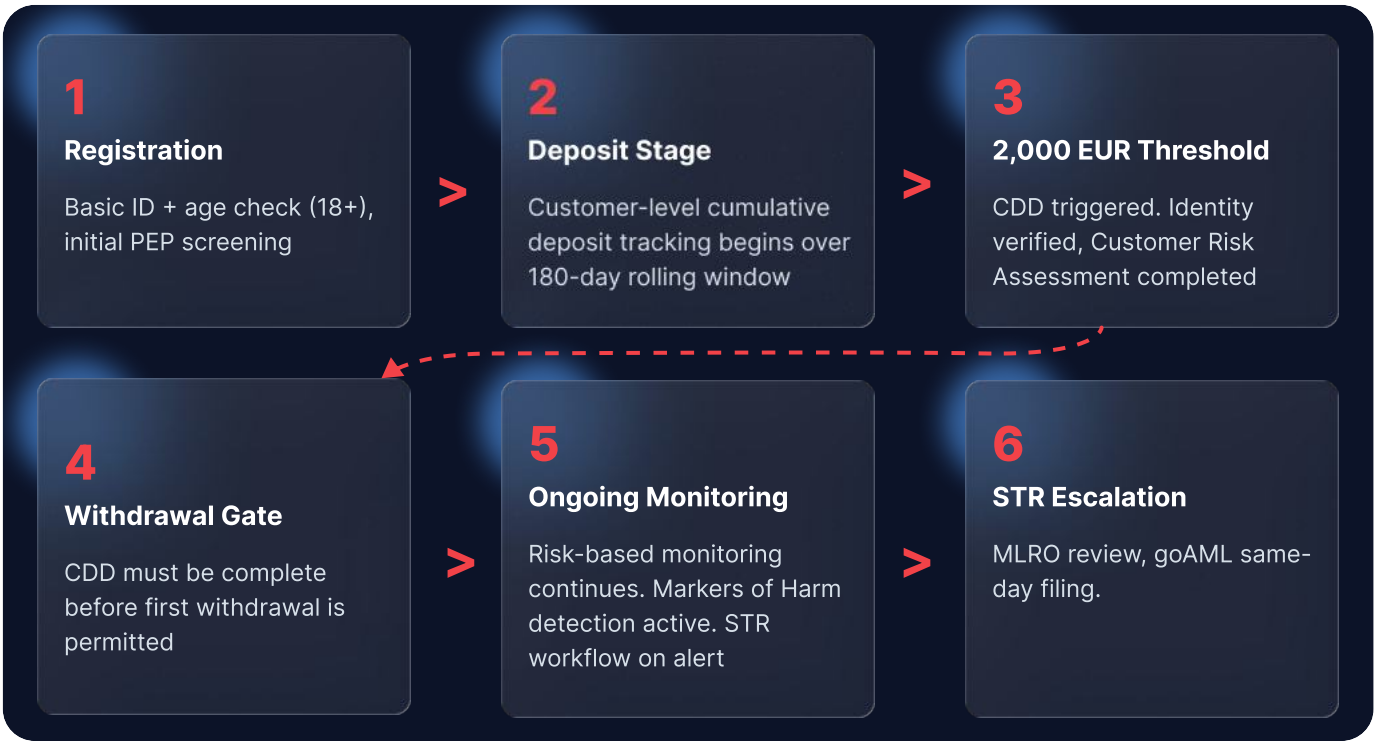
Stanleybet Retail Issue	Online Operator Equivalent
Multiple betting shops	Multiple brands, skins, products, or platforms
Staff recognise customers by sight	CRM and account-level silos with no cross-product link
Per-shop transaction tracking	Per-product or per-wallet tracking
Missing customer-level cumulative view	Fragmented identity, payment, and gaming data

This is the commercial centre of Malta's iGaming compliance risk in 2026. Operators with technically correct individual product controls but no cross-product customer data architecture face the same enforcement exposure as Stanleybet.



The Player Journey Compliance Map

Compliance obligations in Malta gaming are triggered at specific points in the player lifecycle, not as a single process at registration. The architecture question is not about the existence of controls. It is about the data behind them: do the systems have what they need at the moment a trigger fires?



Registration: Basic KYC and Age Check

At account creation, operators should collect full name, date of birth, address, and a government-issued identity document. Age verification (minimum 18 years under the Gaming Act) is mandatory.

PEP and sanctions screening should be applied in line with the operator's AML framework and before the relevant CDD control point. Basic KYC at registration is the foundation for CDD, not CDD itself. The CDD obligation triggers later based on customer activity.

Deposit Stage: Cumulative Tracking Begins

Every deposit must be logged and aggregated at the customer level over a 180-day rolling period across all products, brands, and outlets. This is where the Stanleybet failure originated. The system must aggregate deposits per customer, not per transaction, not per day per outlet, and not per product silo.[10]

[10] FIAU Implementing Procedures Part II for the Remote Gaming Sector : cumulative threshold requirements. September 2020. fiau.org.mt

Withdrawal Control Gate: CDD Completion Required

The customer cannot withdraw until the required CDD information and documentation have been obtained. This is not automatically an Enhanced Due Diligence event for all customers. EDD applies where the Customer Risk Assessment identifies high risk, where the customer is a PEP, or where suspicious activity has been detected. For standard-risk customers who have met CDD requirements, withdrawal proceeds with CDD documentation confirmed.

Ongoing Monitoring

After the first withdrawal, monitoring continues on a risk-based approach. All players are subject to Markers of Harm detection under the MGA Player Protection Directive. High-risk players are monitored with greater frequency. Risk reassessment is required when material changes occur: unusual deposit patterns, new geographies, adverse media, or regulatory triggers.

STR Escalation

When an MLRO determines that knowledge or suspicion of money laundering or terrorist financing exists, an STR must be submitted to the FIAU on the same day. The internal reporting obligation requires employees to report suspected activity to the MLRO no later than the next working day from detection.[11]

[4] FIAU Implementing Procedures Part II for the Remote Gaming Sector : STR escalation. September 2020. fiau.org.mt

The €2,000 CDD Threshold: How to Track, Trigger, and Evidence It

The €2,000 cumulative deposit threshold is the single most operationally consequential compliance obligation in Malta gaming. It is also the one most commonly misunderstood at the architectural level.

What the Threshold Actually Requires

FIAU Implementing Procedures Part II for the Remote Gaming Sector requires operators to conduct Customer Due Diligence and a Customer Risk Assessment by no later than the player's first withdrawal, or when cumulative deposits over any 180-day rolling period reach €2,000, whichever is earlier.[12]

Three architectural requirements follow from this. First, the tracking is customer-level, not transaction-level or outlet-level. Second, the rolling period is 180 days, not a calendar month or a fixed period from account creation. Third, if the customer does not provide the required CDD information or documentation within 30 days of the threshold being reached, the customer relationship must be terminated.

Threshold Calculation Example

Date	Deposit	Product / Outlet	180-Day Total	Action Required
Day 1	€500	Retail sportsbook	€500	Monitor
Day 32	€700	Online casino	€1,200	Monitor
Day 74	€400	Online sportsbook	€1,600	Monitor
Day 91	€300	Retail shop	€1,900	Monitor
Day 103	€200	Live gaming	€2,100	CDD trigger fires: Customer Risk Assessment required. CDD must be complete by the first withdrawal or Day 133 (30 days), whichever is earlier.
Day 181	Any	Any	Day 1 deposit exits window	Recalculate running total

[12] Recalculate running total

Note: If the customer requests a withdrawal before CDD is complete, the withdrawal must be held. If CDD documentation is not obtained within 30 days of the threshold, the customer relationship must be terminated per FIAU Procedures Part II.

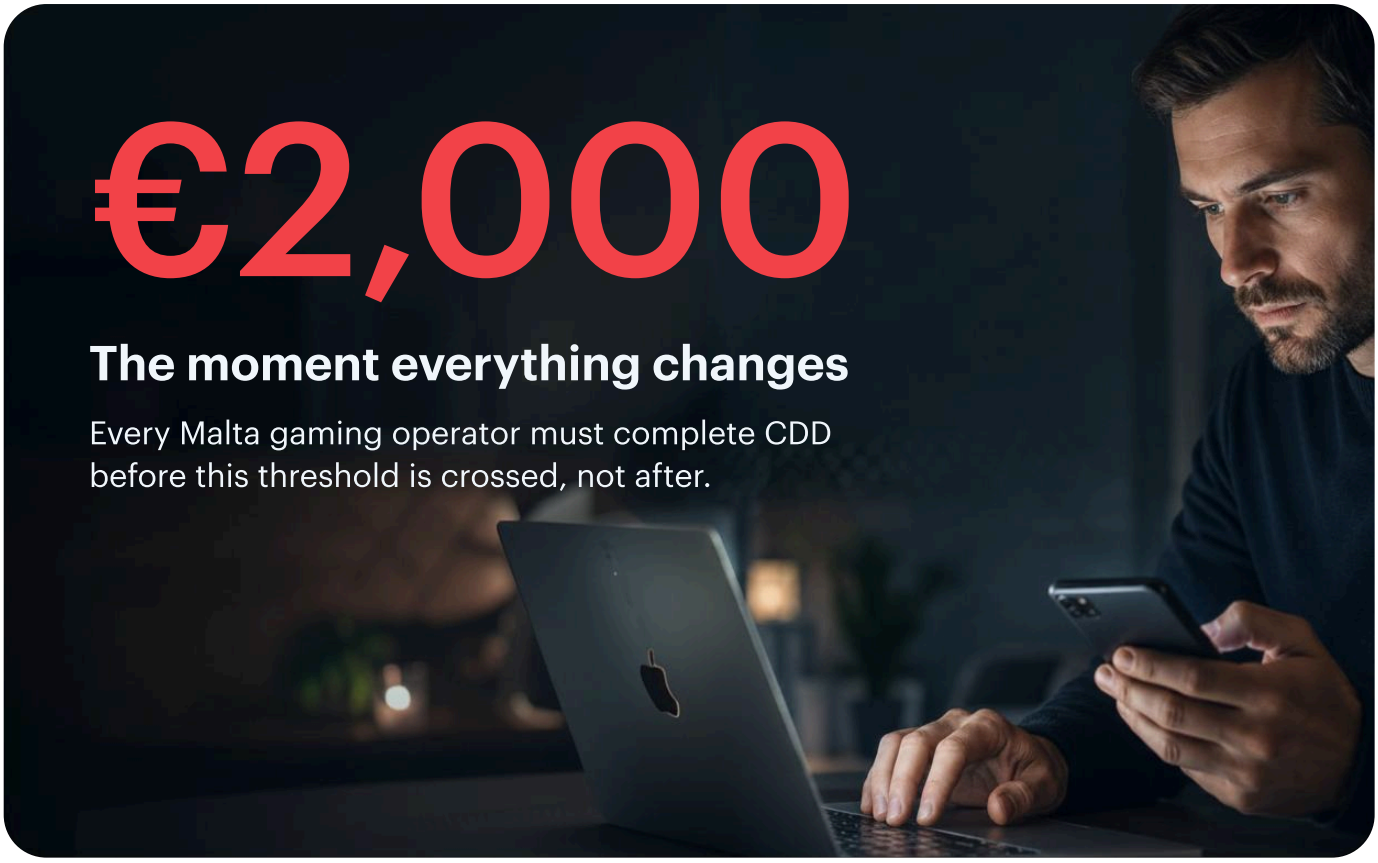
Evidence Operators Should Prepare

For the €2,000 threshold, an examiner may request the following evidence:

- A customer-level deposit ledger showing the cumulative total across relevant products, brands, channels, and outlets over the preceding 180 days at the time CDD was triggered
- The date the €2,000 threshold was reached and the calculation basis
- The date CDD was initiated, and which documents were requested
- The date CDD was completed, or the date the account was terminated, if documentation was not provided
- The Customer Risk Assessment result and the criteria applied

An operator cannot satisfy this with per-product transaction logs in separate systems. The evidence must be presentable as a unified customer record.

Compliance teams evaluating how their current platform architecture handles customer-level threshold tracking across every product and channel can walk through the platform configuration with the Shufti team before committing to a decision.



CDD vs EDD: What Actually Applies and When

One of the most consequential misunderstandings in Malta gaming compliance is conflating the €2,000 threshold with an automatic Enhanced Due Diligence requirement. The threshold triggers Customer Due Diligence and a Customer Risk Assessment. EDD is a separate, higher-intensity obligation that applies only in defined circumstances.

The Distinction That Matters

Obligation	MGA	FIAU
Customer Due Diligence (CDD)	At the €2,000 cumulative deposit threshold, before the first withdrawal	AML/CFT supervision & STR receipt
Enhanced Due Diligence (EDD)	CDD reveals a high-risk customer; the customer is a PEP; suspicious activity detected; any other high-risk indicator under FIAU Procedures	All CDD documentation, plus enhanced identity verification, full address verification, source of funds documentation, and ongoing enhanced monitoring

EDD is triggered by the risk outcome of CDD, not by the deposit threshold itself. A customer who reaches €2,000 in deposits but is assessed as standard risk, is not a PEP, and has no suspicious transaction indicators, undergoes CDD and a Customer Risk Assessment. That is the full obligation for that customer at that control point.

Customer Due Diligence (CDD)

When it applies:

At the 2,000 EUR cumulative deposit threshold OR before the first withdrawal, whichever is earlier.

What it requires:

- Full identity verification
- Document check
- Customer Risk Assessment (CRA)
- Source confirmation if required

Enhanced Due Diligence (EDD)

When it applies:

When CDD reveals high-risk customer, PEP status identified, suspicious activity detected, or any high-risk indicator under FIAU Procedures.

What it requires:

- All CDD documentation
- Enhanced identity verification
- Full address verification
- Source of funds documentation
- Ongoing enhanced monitoring

Player Segment Verification Routing

Not all players follow the same compliance path. The table below maps Malta's five principal player segments to their verification route, CDD trigger, EDD status, and applicable regulatory obligation. Compliance and product teams can use this as an operational routing reference when designing onboarding workflows or reviewing risk tier configurations.

Player Segment	Verification Route at Onboarding	CDD Trigger	EDD Status	Applicable Obligation	Shufti Capability
Standard EU player (standard risk)	Document verification + liveness at registration	€2,000 cumulative deposits over any 180-day rolling period	EDD only if Customer Risk Assessment result = high risk	PMLFTR; FIAU Implementing Procedures Part II	Document Verification + Face Verification
High-volume or VIP player	Document + liveness + proactive Customer Risk Assessment at onboarding	Reached earlier due to deposit velocity; CRA should be completed proactively	Yes: source-of-funds documentation required; senior management sign-off for PEPs	PMLFTR; FIAU Implementing Procedures Part II	Document Verification + Face Verification + User Risk Assessment
Politically Exposed Person (PEP)	Document + liveness + PEP screening flag at onboarding or identified during the relationship	€2,000 threshold (or earlier if identified at registration)	Mandatory and unconditional, regardless of CRA outcome	PMLFTR Art. 16; FIAU Implementing Procedures Part II	AML Screening (1,700+ PEP databases) + Document Verification
Player from a FATF high-risk or monitored jurisdiction	Document + liveness + enhanced geographic risk scoring	€2,000 threshold; geographic risk factor elevates CRA score toward high-risk	Likely: high-risk CRA outcome expected; EDD triggered by CRA result	PMLFTR; FIAU Implementing Procedures Part II	Document Verification (240+ countries) + AML Screening
Corporate or B2B affiliate relationship	Entity verification (KYB) + UBO identification + AML screening on UBOs	Standard CDD threshold for legal persons; UBO-level assessment required	Yes, if any UBO is PEP or high-risk, entity structure complexity may require enhanced review	PMLFTR; Gaming Act Chapter 583	Business Verification + AML Screening

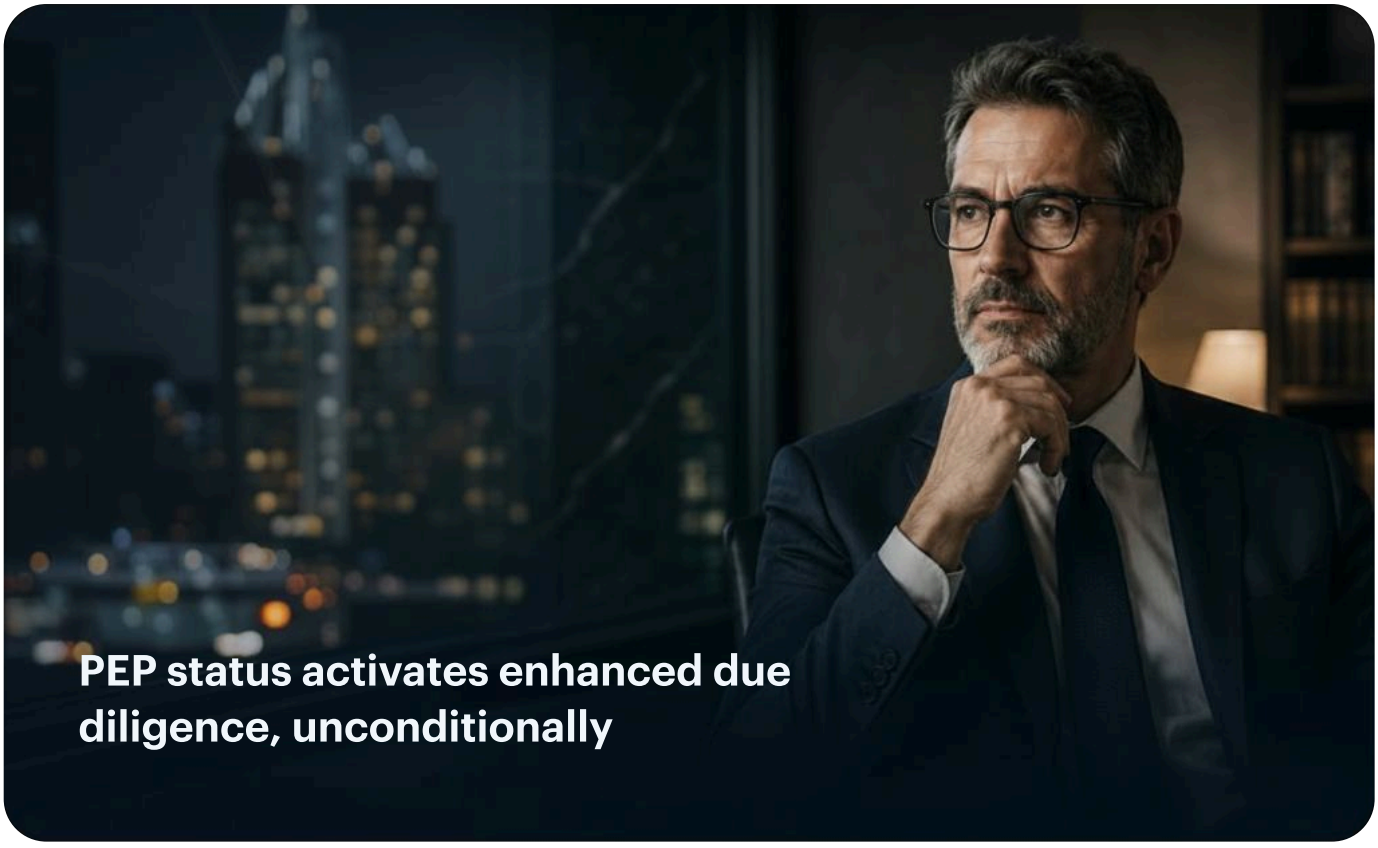
The PEP Trigger: Unconditional

If a customer is identified as a Politically Exposed Person at any point, EDD applies regardless of their Customer Risk Assessment outcome. PEPs include current and former government officials, senior executives of state-owned enterprises, senior military and judiciary officials, and executives of major international organisations. Former PEPs remain subject to EDD for a period determined by risk assessment.

Source of Funds and Source of Wealth

For EDD-triggered customers, operators must obtain documentation supporting the source of funds used in the gaming relationship and, for high-risk or VIP customers, the customer's broader source of wealth. The documentation required is determined by risk assessment and may include bank statements, payslips, tax returns, business sale agreements, inheritance documentation, or other evidence appropriate to the customer's declared financial profile. The requirement is risk-based and proportionate to the level of risk identified.

VIP customers who reach EDD thresholds present a specific operational challenge: high-value players represent disproportionate revenue but also trigger heightened compliance obligations faster due to deposit velocity. Operators must establish clear documented protocols for VIP EDD, including the point at which source-of-funds documentation is required, who approves exceptions, and how refusals are escalated to the MLRO.



[4] FIAU Implementing Procedures Part II for the Remote Gaming Sector : STR escalation. September 2020. fiau.org.mt

CDD vs EDD: What Actually Applies and When

Fraud in iGaming is not a separate problem from AML compliance. Fraud-enabled identity failures directly create CDD exposure.

An operator whose liveness check is defeated by a deepfake has accepted a fraudulent identity. Under FIAU CDD obligations, the operator bears responsibility for the adequacy of its verification process. The use of a third-party IDV vendor does not transfer that liability to the vendor.

Deepfake and Synthetic Identity Fraud

Deepfake and presentation attack fraud against iGaming platforms has escalated sharply as generative AI tools have become more accessible. Operators whose liveness and document verification systems cannot detect synthetically generated identities face direct CDD adequacy failures under FIAU Implementing Procedures Part II.[13] A liveness check that cannot distinguish a live person from a deepfake-generated image is not a player experience issue. It is a CDD adequacy issue with direct FIAU enforcement exposure.

Advanced liveness solutions combine behavioural biometric analysis, document forensics, and presentation attack detection (PAD) certified under independent testing standards such as iBeta PAD Level 1 and 2.

Bonus Abuse and Multi-Accounting

Bonus abuse accounts for a disproportionate share of iGaming fraud incidents.[14] Fraudsters create multiple accounts using synthetic or stolen identity documents, claim welcome bonuses and promotional offers across accounts, and withdraw proceeds. Detection requires cross-product customer linking. An operator without a unified customer identity architecture has the same blind spot for multi-accounting as for cumulative CDD threshold tracking.

[13] FIAU Implementing Procedures Part II for the Remote Gaming Sector : identity verification adequacy obligations. September 2020. fiau.org.mt
[14] Cybersource iGaming Fraud Report 2024. cybersource.com

Account Takeover Fraud

Account takeover (ATO) via credential stuffing exploits password reuse across gaming and other platforms. ATO creates both fraud loss and AML exposure: if a fraudster controls a legitimate player's account and conducts suspicious transactions, those transactions may generate STR obligations. The MLRO may not know the account is compromised at the time of review, creating a systemic monitoring risk.

Mule Accounts and Smurfing

Malta's National Risk Assessment identifies mule account networks as a specific threat to the Maltese gaming sector.[15] Mule accounts are opened to deposit, transfer, and withdraw illicit funds through the gaming platform's multi-payment-method environment. Detection requires cross-product activity monitoring, unusual geographic patterns, and payment method velocity checks.

Operators assessing how their current fraud controls align with FIAU CDD adequacy expectations can request a demo from the Shufti team.

[15] Malta National Risk Assessment. Financial Intelligence Analysis Unit. fiau.org.mt

Markers of Harm Monitoring

The MGA's Player Protection Directive, as amended with implementation obligations taking effect under its transitional provisions, requires operators to monitor for Markers of Harm across active accounts and respond within documented procedures. For high-volume operators, near-real-time automated detection is a practical necessity.

The Mandatory Indicators

Mandatory Marker	Monitoring Requirement
Amount and/or frequency of deposits and wagers	Unusual increases relative to player history; rapid successive deposits or wagers
Multiple payment methods	Multiple payment instruments used within a short period
Reversal of pending withdrawals	Reverse-then-redeposit patterns
Communication-based indicators	Player communications indicating distress, impaired judgement, or problem gambling behaviour
Use of responsible gaming tools	Self-exclusion requests, deposit limit changes, session time limits set or removed

Operators may define additional operator-specific markers appropriate to their product mix and player demographic, such as device access patterns, unusual geolocation, or stake escalation. These are supplementary; the mandatory markers must be monitored regardless of any additional indicators.

Detection Architecture

Real-time automated detection is operationally necessary for any operator with more than a few thousand active players. Manual review cannot process the volume of player interactions required to identify Markers of Harm as they occur. When a Marker of Harm is detected, operators must have a documented response protocol: initial alert, MLRO or responsible gaming officer review, player interaction record, and an action decision.

Responsible Gaming and AML Interaction

Markers of Harm monitoring sits at the intersection of player protection and AML compliance. A player displaying Markers of Harm may also be exhibiting patterns consistent with a mule account or money laundering activity. The MLRO and responsible gaming teams must share information on flagged accounts to avoid treating symptoms of the same underlying issue as separate matters.

Suspicious Activity and STR Workflows

Suspicious Transaction Reports are the primary communication channel between MGA-licensed operators and the FIAU. The same-day submission requirement, tightened in September 2020, is one of the most demanding operational compliance obligations in Malta gaming.

The Same-Day Submission Requirement

Before September 2020, STRs could be submitted within five working days. Under current FIAU procedures, STRs must be submitted on the same day the MLRO determines that knowledge or suspicion of money laundering or terrorist financing exists. For complex cases, submission must occur "within the shortest time possible and without undue delay."[16] The internal reporting obligation requires employees to report suspected activity to the MLRO no later than the next working day from detection.

Red Flag Indicators

FIAU Implementing Procedures Part II specifies patterns that should trigger STR consideration:

- Rapid deposit and withdrawal cycles with minimal or no gaming activity
- Deposits clustering just below €2,000 (structuring indicator)
- Multiple payment methods on a single account within a short period
- Geographic inconsistency between declared residence and transaction IP
- Sudden large deposits inconsistent with prior transaction history
- Account access from new devices or geographies outside the player's normal pattern
- Withdrawal reversal patterns consistent with Marker of Harm indicators

[16] FIAU Implementing Procedures Part II for the Remote Gaming Sector : STR submissithe on deadline. September 2020. fiau.org.mt

MLRO Operational Requirements

A single MLRO managing hundreds of thousands of active players cannot manually review every potential red flag within hours. Automated transaction monitoring systems score suspicious activity and queue flagged cases for MLRO review. The MLRO must also document the reasoning behind every decision to file or dismiss. A dismissed suspicion that is not documented is as much an audit risk as a missed filing.

Tipping-Off Prohibition

Operators cannot notify a customer that an STR has been filed about them. The tipping-off prohibition extends to all staff with knowledge of the filing. Responsible gaming interactions and player communications must not, directly or indirectly, disclose the existence or content of an STR.

Evidence to Prepare for an FIAU Examination

The table below outlines the evidence MGA-licensed operators should prepare for an FIAU AML/CFT examination. In 2024, AML/CFT controls were reviewed through 43 new examinations, while 60 examination reports were completed across MGA/FIAU examination activity.[17] Operators who cannot produce this type of evidence on request face greater enforcement exposure.

Control Area	Evidence the Operator Must Produce
Customer identity	Verification records: document check result, liveness result, timestamp, and audit trail for every customer at the CDD stage
€2,000 threshold	Customer-level deposit ledger across relevant products, brands, channels, and outlets; threshold calculation log; date threshold was reached; date CDD was initiated
CDD completion	Documents requested, documents received, date of completion, Customer Risk Assessment result and criteria applied
PEP and sanctions screening	Screening date and method, match logic applied, false-positive resolution decisions and reasoning, and re-screening schedule
EDD (where applicable)	Source-of-funds documentation received, risk-based rationale for documentation type requested, senior management approval for PEP relationships
STR workflow	Internal suspicion report, MLRO decision log (file or dismiss with reasoning), goAML filing reference and timestamp for filed STRs
Ongoing monitoring	Alert rule configuration, risk-score change history, Markers of Harm trigger log, player interaction record where harm was detected
Record retention	Retention schedule, documented basis for retention periods, evidence that records are held for the required minimum period under PMLFTR

This is the minimum evidence set. Operators who can produce all of the above will be in a materially stronger position than those who rely on narrative explanations of policies without underlying data to support them.

[17] MGA Annual Report 2024, AML/CFT examination statistics. mga.org.mt/publications

Vendor Evaluation Scorecard for Malta iGaming KYC

Vendor selection is a compliance decision. The operator remains liable for the adequacy of its KYC and AML controls regardless of which technology provider delivers them.

The scorecard below translates Malta's specific regulatory requirements into evaluation criteria. Score each vendor 0 to 5 per criterion. A vendor scoring below 3 on any mandatory row should not proceed to the final evaluation.

#	Evaluation Criterion	Regulatory Basis	Score (0–5)	Evidence Required
1	Customer-level deposit aggregation across all products, brands, and outlets	FIAU Procedures Part II; Stanleybet enforcement signal		API documentation + threshold calculation demo
2	Automated CDD trigger at €2,000 cumulative threshold with configurable 180-day window	FIAU Procedures Part II		Workflow configuration demo
3	Document verification covers every jurisdiction the operator accepts players from, with authenticity checks (MRZ, security features, tamper) per document type	PMLFTR Reg. 7(1)(a); FIAU Procedures Part II		Coverage list (country + document type + checks), mapped to operator's accepted markets
4	Liveness/PAD conformant with ISO/IEC 30107-3 (e.g., iBeta Level 1 minimum; Level 2 for high-risk segments)	PMLFTR Reg. 7(1)(b); FIAU Procedures Part II (remote onboarding)		ISO/IEC 30107-3 PAD test report from an accredited lab (current, with PAD level + scope)
5	Synthetic identity document detection	PMLFTR Reg. 7(1)(b); FIAU Procedures Part II		Test results or third-party validation
6	AML screening: EU Consolidated, UN Consolidated, Malta NIIA, PEPs, and adverse media (OFAC where US-touching exposure exists)	PMLFTR; FIAU Procedures Part II §4.4		Itemised watchlist coverage with named source + update frequency per list
7	PEP re-screening on a risk-based schedule post-onboarding	FIAU Procedures Part II: Ongoing Monitoring		Re-screening workflow documentation
8	Markers of Harm detection and automated alerting	MGA Player Protection Directive		Alert rule configuration options
9	MLRO reporting dashboard with STR workflow support	FIAU same-day STR deadline		Dashboard demonstration

[2] FIAU Implementing Procedures Part II for the Remote Gaming Sector : STR submissithe on deadline. September 2020. fiau.org.mt

10	Multi-accounting detection via device fingerprinting	PMLFTR Reg. 8 (ongoing monitoring); FIAU Procedures Part II §5; MGA PPD (self-exclusion bypass)		Technical specification
11	Audit trail logging with evidence retention	PMLFTR record-keeping; FIAU examination readiness		Sample audit report
12	GDPR-compliant cross-border data handling	GDPR Article 28; Malta Data Protection Act 2018		DPA template and transfer mechanism documentation
13	API and SDK integration options	Operational (not regulatory)		Integration documentation
14	Private cloud or on-premise deployment option	GDPR Articles 44–49; Malta Data Protection Act 2018		Deployment architecture documentation
15	ISO 27001 certification (current)	GDPR processor security obligation		Certificate with expiry date
16	Age verification integrated with document and biometric checks	Gaming Act Chapter 583; MGA Player Protection Directive (minimum age 18)		Workflow demonstration
17	AMLR 2027 readiness roadmap	AMLR direct application from 10 July 2027		Product roadmap statement
18	SLA for regulatory examination support	PMLFTR Reg. 11 (record availability on request); FIAU Procedures Part II		SLA documentation

Red flag: A vendor that confirms “AML screening” but cannot show PEP re-screening logs, alert timestamps, and MLRO decision workflow evidence may not have sufficient AML monitoring evidence for Malta gaming compliance workflows. Confirm capability with evidence, not with sales claims.

Operators building an RFP from this scorecard, or assessing how a current provider maps against Malta’s post-Stanleybet requirements, can configure and price a full stack directly at any tier.

Implementation Blueprint: 30/60/90 Days

Compliance remediation after the Stanleybet enforcement signal requires a structured programme, not a technology purchase. The 90-day blueprint below addresses the highest-enforcement-risk gaps first and works outward to operational readiness.

Days 1-30

Audit and Prioritise

The assessment in the first 2 weeks should cover:

- Does the platform produce a single deposit ledger per customer across every product and outlet for the preceding 180 days?
- Is the €2,000 CDD threshold tracked at the customer level, not the outlet or transaction level?
- Does the CDD trigger automatically fire when the threshold is reached?
- Can the MLRO demonstrate same-day STR submission compliance with a decision log for every filed and dismissed suspicion?
- Does Markers of Harm monitoring include all five mandatory MGA indicators?

Weeks 3-4: Map self-audit findings to regulatory obligations. Prioritise by enforcement risk: cross-product customer data architecture first, then CDD trigger automation, then STR workflow timing, then Markers of Harm completeness.

Days 31-60

Vendor Selection and Planning

Weeks 5-7: Issue RFP to 3-5 vendors using the 18-criterion scorecard. Do not advance a vendor that cannot demonstrate customer-level deposit aggregation, iBeta-certified liveness, PEP re-screening, and MLRO workflow support with evidence.

Weeks 7-9: Technical scoping. Define integration points between the selected verification stack and the gaming platform. Confirm data flow for customer-level deposit events from every product into the threshold calculation system.

Days 61-90

Implementation and Validation

Weeks 10-12: Parallel run. Integrate the new verification stack while running existing systems in parallel. Validate customer-level threshold detection accuracy, deepfake detection, PEP screening match rate, and STR automation timing.

Weeks 12-13: Staff training. Brief compliance, customer service, and fraud teams on new workflows. MLRO briefing on updated decision-log requirements and same-day STR process.

Week 13-14: Cutover and KPI baseline. Full cutover. Establish baseline: no CDD tracking failures, STR average submission time within deadline, 100% PEP screening coverage at CDD. Given the volume of AML/CFT examination activity reported in 2024, mid-to-large MGA operators should prepare as though their controls may be reviewed.

About Shufti

Shufti is a global identity verification and AML screening platform serving 2,000+ enterprise customers across financial services, iGaming, healthcare, and other regulated industries in 240+ countries and territories. The platform combines document verification, face verification, age assurance, AML screening, device intelligence, and risk assessment in a single integrated system, deployable via API, SDK, or no-code workflow editor.

Document Verification covers 10,000+ document types across 240+ countries with 150+ OCR languages. Face Verification is iBeta PAD Level 1 and Level 2 certified for presentation attack detection. AML Screening integrates 1,700+ watchlist sources with 15-minute update cycles.

Deployment options include SaaS, Private Cloud, and On-Premise, addressing data residency requirements for heavily regulated operators. Certifications include ISO 27001, SOC 2 Type II, and GDPR compliance.

How Shufti Maps to Malta Gaming Controls

Control Obligation	Shufti Capability	Evidence Produced
Customer identity at CDD trigger	Document Verification (10,000+ types, 240+ countries) + Face Verification (iBeta PAD Level 1 & 2)	Verification timestamp, document result, liveness result, audit log
PEP and sanctions screening	AML Screening (1,700+ watchlist sources, OFAC, UN, EU, FATF, 20M+ records, 15-min updates)	Screening date, match logic, false-positive resolution
Deepfake and synthetic ID detection	Face Verification with iBeta PAD; Document Verification with zero-shot AI	PAD test result, document authenticity log
Multi-accounting and mule detection	Device Intelligence (device fingerprinting, VPN/proxy detection, emulator detection)	Device fingerprint log, velocity alerts, linked account flags
Markers of Harm and Risk Scoring	User Risk Assessment (configurable rules engine, real-time risk scoring)	Alert timestamp, risk score history, trigger rule applied
MLRO workflow and STR support	MLRO dashboard with configurable alert queues and workflow routing	Decision log, queue timestamp, escalation record
FIAU examination evidence	Audit trail logs for verification, AML screening, risk scoring, and MLRO decisions, covering all Shufti-processed events	Exportable audit report per customer for Shufti-processed events
Data residency and GDPR	SaaS, Private Cloud, and On-Premise deployment; ISO 27001; GDPR-compliant processing	DPA documentation, transfer mechanism records

Note: Deposit aggregation, Markers of Harm workflows, STR workflow routing, and cross-product audit trails depend on integration with operator transaction, player activity, and case-management systems. Shufti supports these workflows when the relevant operator data is connected and configured.

Operators can review Malta iGaming compliance coverage and deployment options, or build and price a plan directly.

Shufti is a technology and tools provider. The platform supports operators in building and evidencing their compliance controls. Shufti does not provide legal or regulatory advice.

Shufti

Verify Malta iGaming Players with Controls Built for FIAU Examination

Shufti's document verification, liveness detection, and AML screening can be configured to support Malta iGaming CDD threshold triggering, PEP screening, Markers of Harm monitoring, and audit trail requirements. Request a demo to see it running in an MGA-licensed operator workflow.

Book a Malta iGaming KYC Demo Now

shuftipro.com
sales@shuftipro.com