Shufti

Cyprus

GUIDE

CySEC Forex KYC Compliance Handbook

A Practical Toolkit for Document Verification, Multi-Script Onboarding, and Audit-Ready KYC at Cyprus Investment Firms

VÉRIFICATION D'ÂGE KJM

PCI DSS

iBeta Niveau 1

ISO 27001: 2013

CE+

QG GDPR

SOC2

GDPR

CCPA

Executive Summary

Cyprus Investment Firms face a KYC environment that few other EU licensing jurisdictions match in complexity. High-volume cross-border onboarding, a client base concentrated in non-Latin-script markets, post-December 2024 RCOS obligations, and active CySEC audit activity combine into a compliance burden that generic onboarding infrastructure was not built to absorb.

The challenge is no longer proving that remote onboarding can happen. Since CySEC's RCOS framework entered application on December 1, 2024, the question audit teams assess is different: can the firm produce the evidence?

Liveness records, document verification logs, AML screening trails, EDD files, and annual rescreening records must be present, dated, retrievable, and customer-specific. For firms with Russian, MENA, Indian, or Nepali client exposure, those records must also demonstrate that script-aware verification and name-matching controls are in place.

This handbook gives AMLCOs, MLROs, Heads of Compliance, and Risk Officers the tools to assess and improve their position. Inside: a Cyprus client risk map segmenting four onboarding tiers; a nine-row CySEC Audit Evidence Matrix linking each compliance area to required evidence, severity, and remediation; a multi-script verification breakdown for Cyrillic, Arabic, and Devanagari documents; a scored vendor evaluation scorecard; a 30-day remediation plan; and a one-page evidence pack template ready for audit preparation.

The firms that will hold up best under CySEC review are those that have built a connected evidence layer, not those that have simply deployed a verification tool.

Table of Contents

Shufti

CySEC's 2024 Enforcement Activity

Cyprus Investment Firms no longer need to prove that remote onboarding is technically possible. Since December 1, 2024, the question CySEC audit teams ask is if remote onboarding is controlled, risk-assessed, and auditable. The RCOS framework introduced by Policy Statement PS-01-2024 and Directive RAD 282/2024 has been in application for over a year. Firms that implemented the framework are now subject to audit review.

€2.12 Million

in administrative fines imposed on Cyprus Investment Firms by CySEC in 2024

The 850+ audits conducted in 2024 signal that every CySEC-supervised firm faces a material probability of review within a 12-month window. The question is not if, but when. The more pressing question is if the evidence will hold up.

In 2024, CySEC conducted more than 850 on-site and remote thematic audits and imposed approximately €2.76 million in total administrative fines, including €2.12 million against Cyprus Investment Firms. CySEC also requested corrective measures in 321 cases and instructed more than 70 supervised entities to implement specific measures to fully comply with AML Law and Directive obligations.

For forex and CFD operators, the audit environment is sharper than for most CySEC-licensed entities. High-volume cross-border onboarding introduces Cyrillic, Arabic, and Devanagari identity documents, sanctions-adjacent client profiles, transliteration inconsistencies, and manual-review pressure that generic compliance infrastructure cannot absorb without creating audit exposure.

This handbook addresses the three operational dimensions that determine audit outcomes for Cyprus CIFs: multi-script document verification across Cyrillic, Arabic, and Devanagari documents; liveness detection evidence that satisfies PS-01-2024 expectations; and audit trail construction that allows CySEC auditors to reconstruct every onboarding decision.

What Changed: PS-01-2024, RAD 282/2024

The December 1, 2024, application date for CySEC's RCOS framework did not end the compliance cycle. It began the audit cycle. Firms that spent 2024 implementing liveness detection, filing RCOS notifications, and updating risk assessments must now demonstrate that those controls are documented, consistent, and auditable.

Aug 6, 2024

PS-01-2024 and RAD 282/2024 published. RCOS framework clarified: liveness required for unattended onboarding.

Dec 1, 2024

New RCOS rules enter application. Unattended RCOS must include liveness detection. No deposit ceiling.

2025 onwards

CySEC audit review period begins. Firms must evidence controls, not just implementation.

The Core Regulatory Shifts

RAD 282/2024 replaced the previous video-call derogation framework, which permitted remote onboarding under a €2,000 annual deposit ceiling per customer. The new directive removes that ceiling and applies a technology-neutral RCOS framework to all customer types. Firms choose their own RCOS method, conduct a documented risk assessment, notify CySEC in advance (an informational notification, not an approval process), and deploy before the application date.

PS-01-2024 clarified the evidentiary standard for unattended RCOS. For onboarding journeys without human staff interaction, liveness detection is required. A static selfie alone does not evidence that a live person was present at the point of capture, which is the standard CySEC audit teams apply when examining the verification record.

What Audit Teams Examine

CySEC audit teams examining RCOS implementations after December 2024 are likely to focus on four areas:

1. If a documented risk assessment for the chosen RCOS method exists and is board-approved or compliance-approved
2. If CySEC notification evidence is retained in firm records
3. If liveness detection records (timestamped, with method and outcome logged) are stored in each customer file
4. If the RCOS risk assessment has been reviewed following implementation

The notification is informational. CySEC does not approve RCOS methods in advance. The regulatory risk sits with the firm's choice of method and its ability to demonstrate that the choice was appropriately risk-assessed.

Cyprus CIF Onboarding Risk Map

Cyprus has one of the EU's highest shares of foreign nationals as a proportion of its resident population: reported at approximately 24.8% as of January 2025, according to Eurostat. Russian nationals represent approximately one in five foreign residents in Cyprus, making them the largest single non-EU national group by population.

For Cyprus Investment Firms, this creates a practical onboarding challenge: customer files regularly involve Cyrillic, Arabic, Devanagari, and Latin-script identity documents, plus sanctions and PEP screening across multiple name variants in the same compliance workflow.

Client Segment	Common Documents	Script Complexity	Primary Screening Risk	Verification Challenge
Russian nationals/ residents	Passport, residence permit	Cyrillic + Latin via ICAO transliteration	EU sanctions, PEPs, ownership links	Transliteration variants, EDD requirements
MENA clients	Passport, national ID	Arabic: no universal transliteration standard	OFAC, EU, UN list name variants	False positives, manual review burden
Indian/Nepali clients	Passport, national ID	Devanagari: no ICAO standard	Standard AML, PEP screening	OCR accuracy, name-order variants
EU clients	Passport, national ID	Latin script	Standard AML, PEP screening	Lower script complexity
Corporate/ UBO structures	Corporate registration, director IDs	Varies by jurisdiction	Beneficial ownership, PEP, sanctions	UBO identification at 25% threshold

The Four Client Verification Tiers

Tier 1: Standard EU Onboarding

EU nationals presenting Latin-script passports or national identity documents, with no PEP or sanctions exposure. Standard CDD applies under Cyprus AML Law 188(I)/2007.

Tier 2: Non-Latin Script Onboarding

Russian, Indian, Nepali, and some MENA nationals requiring script-aware OCR and transliteration normalisation before sanctions screening can produce reliable results. Standard CDD applies, with elevated manual-review risk if the document verification system lacks native script support.

Tier 3: Sanctions-Adjacent Onboarding

Russian nationals (EU sanctions exposure under Regulation 833/2014 and subsequent amendments), clients from FATF high-risk jurisdictions, and nationals from countries subject to targeted EU, OFAC, or UN sanctions programmes. Risk-based EDD is required, with documented source-of-funds and source-of-wealth assessment where the client profile warrants it.

Tier 4: PEP and Beneficial Owner Identification

Clients identified as politically exposed persons, their close associates, or family members, and corporate clients where ultimate beneficial owners hold 25% or more of shares or voting rights under Cyprus AML Law 188(I)/2007. EDD documentation must include ownership structure, source-of-funds analysis, and periodic reassessment.

The CySEC Audit Evidence Matrix: What Firms Should Be Ready to Produce

CySEC audits are evidence-driven. Audit teams assess if specific documents and records are present, dated, organised, and retrievable. The matrix below maps each compliance area to the evidence firms should be prepared to produce.

Compliance Area	Evidence to Retain	Severity	Remediation Action	Shufti Control
Liveness detection records	Timestamped liveness record per verification: method, outcome, anti-spoofing result, customer ID	Critical	Replace static selfie-only flow with a liveness-capable RCOS implementation	Face Verification with 3D liveness detection (iBeta PAD Level 1 and 2)
RCOS risk assessment	Signed, dated, board or compliance-approved risk assessment; version history if updated	Critical	Prepare risk assessment documenting RCOS method selection rationale and retain in firm records	Workflow documentation; RCOS configuration evidence
CySEC notification evidence	Notification letter or form with acknowledgement retained	Critical	File notification evidence and confirm it is retrievable	RCOS implementation record
Document verification log	OCR result, document type, country, confidence score, decision, date per customer	High	Confirm vendor logs OCR result and confidence score per customer, not just pass/fail	Document Verification with per-verification audit log

AML screening at onboarding	Screening log: lists checked, date, result, match status, override rationale where applicable	High	Add documented name-match workflow and scheduled rescreening cycle	AML Screening across OFAC, EU, UN with override log
EDD documentation	Source-of-funds rationale, ownership structure, risk rating, review date	High	Implement risk-based EDD workflow for Tier 3 and 4 clients	Due Diligence workflow + User Risk Assessment
Annual rescreening records	Rescreening date, lists checked, result, reviewer, escalation decision per customer	High	Implement periodic rescreening schedule documented in internal AML policy	AML Screening (scheduled rescreening)
STR/SAR decision trails	goAML submission record, decision rationale, monitoring rule triggered	High	Ensure every STR/SAR decision references a documented transaction monitoring rule	Transaction Screening and alert log
5-year record retention	Indexed customer file per Cyprus AML Law 188(I)/2007	Medium	Centralise records into a searchable, customer-level, single-export format	Workflow logs + API records export

The Exelcius Prime Ltd enforcement case illustrates the record-production standard. CySEC imposed a €740,000 administrative fine on Exelcius Prime Ltd in August 2024, citing violations including failure to provide required records, inadequate organisational structure, and client-best-interest failures. The case demonstrates that the inability to produce required records on demand is an enforcement risk in itself.

Found gaps in your evidence pack?

Compliance teams can walk through how Shufti maps to each row in this evidence matrix before committing to a vendor decision. Walk Through the Platform

Multi-Script Document Verification: Cyrillic, Arabic, and Devanagari

Multi-script document verification produces the most persistent KYC vulnerability for Cyprus Investment Firms. Russian passports, Arabic national identity documents, and Indian and Nepali passports all require script-aware processing before sanctions screening can proceed reliably. A system that reads these documents without native script support generates false positives during screening, false negatives during name matching, and manual-review burdens that are operationally unsustainable at volume.

Russian Passports and ICAO Cyrillic Transliteration

ICAO Document 9303 defines the international standard for transliterating Cyrillic characters into Latin equivalents for the machine-readable zone of travel documents.

The MRZ field width is fixed at 44 characters per line. A Russian national named "Иванов Иван Александрович" may appear in the MRZ as "IVANOV IVAN ALEKSANDROV" due to the character limit, or as "IVANOV I ALEKSANDROV" in abbreviated form. Both are compliant with ICAO standards and both are valid representations of the same person.

Generic OCR that reads visible printed text, rather than applying ICAO transliteration logic, cannot recognise these as the same entity. A single Russian national generates multiple name variants depending on which document field the OCR engine extracts from, creating false negatives during sanctions screening. RAD 282/2024 requires firms to use a "reliable and independent source" for document verification. The directive does not specify transliteration methodology. The audit liability for false negatives rests with the firm.

Arabic Documents and Transliteration Without a Universal Standard

Arabic introduces a fundamentally different verification problem: no international transliteration standard exists. The Arabic name "محمد" validly transliterates to "Mohammed," "Muhammad," "Mohammad," "Mohamed," "Mehmet," and "Mohd" depending on the phonetic convention used. An Arabic national identity document may present the name in Arabic script alongside a Latin transliteration selected by the issuing authority. That Latin form may differ from the transliteration used by OFAC, the EU consolidated list, or the UN Security Council list.

Note: Arabic name matching requires script-normalised fuzzy matching calibrated to phonetic similarity. A single Arabic name may produce five or more valid transliterations across different sanctions lists.

Devanagari Script: Indian and Nepali Passports

Unlike the Cyrillic-to-Latin MRZ transliteration in Russian passports, Devanagari name romanisation can vary across issuing practices and source systems. There is no equivalent of ICAO Document 9303 for Devanagari. CIFs should verify that their OCR and name-matching workflows can preserve original-script data and manage Latin spelling variants across Indian and Nepali passport populations.

Script	Document Type	Standard	Latin Variant Risk	Verification Challenge
Cyrillic	Russian passport	ICAO Doc 9303 (defined)	**High: MRZ abbreviations produce multiple valid forms**	Name-match false negatives without ICAO-aware OCR
Arabic	National ID, passport	None: phonetic convention varies	**High: 5+ valid variants per name**	Override burden without documented matching methodology

Devanagari	Indian, Nepali passport	No universal standard	**Medium: issuing-office variation**	OCR failures producing corrupted or inconsistent name strings
Latin	EU passports, national IDs	Not applicable	**Low**	Standard verification risk

Real-World OCR Challenges by Script and Their Compliance Consequences

The table below shows how each script creates specific verification and screening challenges, using illustrative examples to show what happens when a generic (non-script-aware) OCR system processes these documents. These scenarios reflect the kinds of issues that compliance teams encounter when their infrastructure lacks native multi-script support.

Script	Common OCR Challenge	Illustrative Example	Compliance Consequence Without Fix
Cyrillic	MRZ field limited to 44 characters per line. Long Russian names are truncated or abbreviated per ICAO Doc 9303.	"IVANOV IVAN ALEKSANDROV" in MRZ vs "Ivanov Ivan Aleksandrovich" on the ID biographic page: both valid, neither an exact match	Without ICAO-aware OCR, a Cyrillic name generates 2-3 valid Latin variants. Each sanctions list entry may use a different form. False negative without fuzzy matching; manual override requires documented rationale per customer
Arabic	No universal transliteration standard: phonetic convention varies by country and document issuer	"Mohammed Al-Otaibi" on a Saudi national ID vs "Muhammad al-Utaibi" on the OFAC SDN list: same person, different transliteration	Without script-normalised fuzzy matching, every Arabic-script client generates potential false negatives. Manual override of each must be documented with case-specific rationale, not a generic “names looked similar” note

Devanagari	Romanisation of Devanagari script varies across issuing offices and document generations. No ICAO standard applies.	"Pramod Kumar Bhattarai" on one Nepali passport vs "Pramoth Kumar Bhattray" on an older reissue for the same person	Without Devanagari-native OCR, the same person across two documents appears as two different individuals in the compliance system. This creates duplicate records, screening gaps, and EDD confusion
Latin	Diacritics in some EU passports (Czech, Polish, Romanian) are dropped inconsistently by generic OCR	"Jan Novak" vs "Jan Novák": both refer to the same Czech national, but string matching fails	Lower risk than multi-script clients, but still creates false negatives for Central and Eastern European nationals on sanctions or PEP lists that retain diacritics

Key insight: CIFs with high volumes of Russian, MENA, Indian, or Nepali clients that lack native script support typically see elevated manual override rates. Override decisions that cannot be justified algorithmically create audit exposure that accumulates per customer.

Shufti's Document Verification supports 10,000+ document types across 240+ countries and territories, with proprietary OCR across 150+ languages, including native Cyrillic, Arabic, and Devanagari processing. Compliance teams assessing if their current verification infrastructure handles these three scripts without manual review escalation can review Shufti's multi-script capabilities and configure a pilot assessment.

Sanctions and PEP Screening Across Name Variants

After document verification extracts a customer's name, that name must be normalised before sanctions screening can produce reliable results. This normalisation pipeline is where most false positives and false negatives originate in multi-script CIF environments.

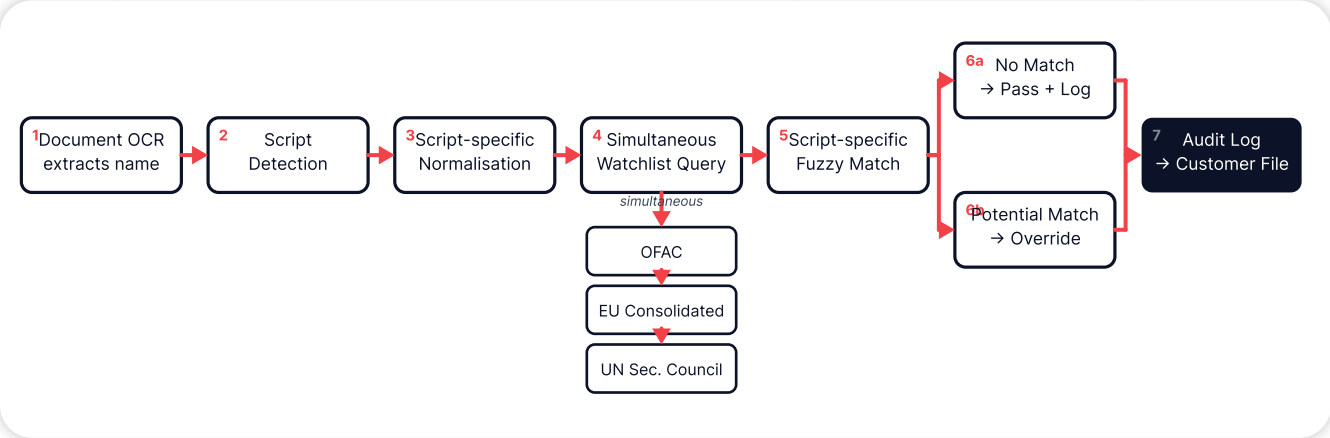
The Name Normalisation Pipeline

Name normalisation before screening involves four sequential operations: diacritics removal; vowel-length normalisation; hyphen and space standardisation; and script conversion from Cyrillic, Arabic, or Devanagari into Latin. After normalisation, fuzzy matching algorithms measure the character edits required to transform one name string into another.

A single global match threshold does not work across all scripts. The thresholds in the table below are illustrative examples only. Firms should document their own calibration methodology, calibrated by script, document type, sanctions-list source, customer risk rating, and false-positive/false-negative tolerance, and maintain QA evidence demonstrating how overrides are reviewed when scores fall in threshold grey zones.

Step	Operation	Script-Specific Consideration	Illustrative Threshold
1	Diacritics removal	Latin: standard; Cyrillic/Arabic: via script conversion first	n/a
2	Script conversion to Latin	Cyrillic: ICAO Doc 9303; Arabic: phonetic normalisation	n/a
3	Fuzzy match: Latin names	Standard European passports	95%+ (example)
4	Fuzzy match: Cyrillic names	ICAO MRZ abbreviations produce multiple valid forms	85–90% (example)
5	Fuzzy match: Arabic names	No universal standard; phonetic variants expected	80–85% (example)
6	Override documentation	Case-specific rationale required; methodology reference mandatory	n/a

Note: Fuzzy matching thresholds are not universal regulatory standards. Firms should document their own calibration methodology and QA evidence. The figures above are illustrative examples only.



Multi-Source Sanctions List Querying

Sanctions lists differ in language coverage and update frequency. OFAC's Specially Designated Nationals list uses Latin-script entries only. The EU consolidated list includes both Latin and original-script entries for many Russian and MENA entities. UN Security Council lists vary significantly by language coverage.

Firms should document their periodic rescreening cadence according to customer risk rating, sanctions exposure, and internal AML policy. Where annual rescreening is used as the minimum control, the customer file should show the date, lists checked, result, reviewer, and escalation decision

PEP Screening Across Script Variants

Politically exposed person screening presents the same multi-script challenge as sanctions screening. A Russian regional official may appear in one PEP database as "Sergei Ivanov" and in another as "Sergey Ivanov." Both are correct Latin representations of the same Cyrillic name. PEP screening without script-aware normalisation generates missed matches that create audit exposure.

Shufti's AML Screening queries 1,700+ watchlist sources, including OFAC, EU consolidated lists, and UN Security Council designations, with records updated every 15 minutes and an average screening response time of 2.32 seconds. The platform maintains documented decision trails for name-match review decisions, producing customer-level audit records.

Enhanced Due Diligence for Sanctions-Adjacent and High-Risk Clients

Standard CDD is insufficient for client profiles that carry sanctions risk, high-risk jurisdiction exposure, or beneficial ownership complexity. CySEC audit teams expect EDD documentation that addresses each risk factor specifically. A generic risk-rating label applied to a customer file does not constitute an EDD record.

Russian Nationals: Individual Risk Assessment

EU Russia sanctions under Regulation 833/2014 and subsequent amendments impose restrictions on specific categories of transactions, entities, and securities: they do not create a blanket prohibition on servicing all Russian national clients. The relevant restrictions cover areas including certain deposit services, crypto-asset services, payment transactions with designated persons, and investment services relating to specified Russian-issued securities.

Note: EU sanctions on Russia do not create a blanket prohibition on servicing all Russian national clients. CIFs should document client-specific sanctions-risk indicators, including nationality, residence, beneficial ownership, source of funds, source of wealth, payment route, and product exposure, not a nationality-based determination alone.

A sanctions-risk assessment for Russian clients should document if the client, beneficial owner, or funding source falls within any designated category; if the product type or transaction structure creates exposure to restricted securities; and if the payment route introduces third-party funding risk. This assessment belongs in the customer file alongside source-of-funds rationale and source-of-wealth documentation where warranted.

MENA Clients: Arabic-Script Screening and High-Risk Jurisdiction Exposure

MENA client bases introduce Arabic-script document verification, transliteration variability, and elevated exposure to sanctions programmes across OFAC, EU, and UN jurisdictions simultaneously. A CIF onboarding a client from a MENA country designated by FATF as high-risk or non-cooperative should treat FATF status as an EDD trigger alongside individual sanctions screening.

MOKAS, Cyprus' Financial Intelligence Unit, received 3,870 Suspicious Transaction Reports and Suspicious Activity Reports in 2024, representing a 62% year-on-year increase. MOKAS reporting reflects heightened detection of sanctions evasion, beneficial ownership masking, and third-party payment routing. Each STR/SAR submission requires a documented decision trail referencing a specific transaction monitoring rule, not ad hoc compliance judgement.

3,870

Suspicious Transaction Reports filed with MOKAS in 2024

+62% year-on-year increase

EDD Evidence Requirements by Risk Tier

Risk Tier	Trigger Criteria	Required Documentation	Minimum Review Cadence
Standard CDD	EU national, low-risk jurisdiction, no PEP or sanctions match	Identity document, CDD assessment, onboarding screening result	Annual relationship review
Elevated CDD	Non-EU national, non-Latin script, no direct sanctions exposure	Standard CDD plus source-of-funds rationale	Annual

EDD: Sanctions-Adjacent	Russian national, MENA national from a high-risk jurisdiction, FATF designation	Standard CDD plus ownership structure, source-of-funds analysis, documented sanctions-risk assessment	Annual minimum; interim on trigger event
EDD: PEP	PEP, close associate, family member	Standard CDD plus EDD, source-of-wealth documentation, senior management approval	Annual

RCOS Liveness Evidence Pack: What CySEC Expects in the Customer File

PS-01-2024 established the evidentiary standard for unattended RCOS. For firms running onboarding journeys without human staff participation, liveness detection is required. The post-implementation audit challenge is not if liveness detection was deployed. It is if the liveness record for each customer is sufficient to evidence that deployment.

What the Liveness Record Must Contain

- **Verification timestamp:** date and time of the liveness check in a retrievable format
- **RCOS method:** the specific method used (facial recognition with anti-spoofing; 3D depth detection; dynamic selfie with biometric freshness check; eIDAS-compliant solution)
- **Liveness outcome:** confirmed live / failed/escalated to manual review
- **Customer identifier:** unique customer reference linking the liveness record to the rest of the customer file
- **Document type and country:** the identity document used in conjunction with the liveness check
- **Face match result:** biometric match score or pass/fail, with the threshold applied documented
- **Anti-spoofing result:** confirmation that presentation attack detection ran as part of the check
- **Fallback action (if applicable):** escalation route, agent review record, or manual determination where liveness could not be confirmed

Control Area	Pre-August 2024 Framework	Post-December 2024 Framework
Remote ID method	Video call with a €2,000 annual deposit limit per customer	RCOS with liveness detection for unattended journeys (no deposit ceiling)
Liveness requirement	Not required: static selfie or no face check acceptable	Liveness detection required: static selfies alone do not evidence live presence
CySEC notification	Not required	Informational notification required before implementation (retained in firm records)
Risk assessment	Not required	Required: must document RCOS method selection rationale and risk controls

Static Selfies and Presentation Attack Risk

Static selfie systems capture a still photograph and compare it against a reference image. They do not confirm that a live person was present at the point of capture. Presentation attacks (printed photographs, video playback, deepfake images, or face-mask attacks) can defeat a static selfie system because the system has no mechanism to detect that it is reviewing a copy rather than a person.

A customer file containing only a static selfie may create audit exposure because it does not evidence a liveness method, a timestamped outcome, or presentation-attack detection. Acceptable liveness technologies under the technology-neutral framework include facial recognition with active anti-spoofing, 3D liveness detection using depth mapping, dynamic selfie requests requiring specific user actions, and biometric freshness analysis.

Shufti's Face Verification uses 3D liveness detection certified to iBeta PAD Level 1 and Level 2 (the anti-spoofing standard for biometric systems), with a 98.22% acceptance rate and a 2.98-second average response time. Verification records include timestamps, liveness outcome, anti-spoofing result, and face match score.

30-Day CySEC KYC Readiness Plan

The plan below gives compliance teams a structured path from gap identification to documented controls, organised around the four areas most closely examined in CySEC audits.

Week 1
Audit Inventory

Week 2
Liveness and RCOS

Week 3
Multi-Script Screening

Week 4
EDD and Rescreening

Week 1: Audit Evidence Inventory

- Conduct a full audit evidence inventory using the matrix in Section 5 as the framework
- For each compliance area, confirm if the required documentation exists, is dated, is retrievable, and is stored in a searchable, customer-level format
- Identify gaps in liveness records, annual rescreening documentation, EDD files, and RCOS risk assessments
- Assign an owner and remediation deadline to each gap

Week 2: Liveness and RCOS Controls

- Review the liveness detection method currently deployed and confirm it produces timestamped records per customer
- Verify that the RCOS risk assessment is current, board or compliance-approved, and that CySEC notification evidence is retained
- If static selfies are the only face-check method, initiate a vendor assessment for liveness-capable alternatives
- Run a spot-check on 20 recent customer files: confirm that each contains a liveness record with timestamp, method, outcome, and customer identifier

Week 3: Multi-Script and Sanctions Screening

- Pull a sample of Russian, MENA, Indian, and Nepali customer files and confirm that OCR extraction quality was logged alongside verification decisions
- Review the AML screening configuration: confirm that OFAC, EU consolidated list, and UN Security Council lists are queried simultaneously

- Confirm that the fuzzy matching calibration methodology is documented with a script-specific threshold rationale
- Audit override decisions in the sample files: verify that each contains a documented rationale specific to the individual match, not a generic override note

Week 4: EDD and Periodic Rescreening

- Review Russian national, Russia-resident, Russia-linked UBO, and Russia-funded client files to confirm that sanctions-risk indicators, source of funds, beneficial ownership, product exposure, and payment routes are documented where relevant
- Run the periodic rescreening cycle for any customers whose last screening date exceeds the firm's documented rescreening cadence
- Confirm that STR/SAR decision trails in customer files reference specific transaction monitoring rules
- Compile the remediation report from all four weeks, update the firm's AML risk assessment, and schedule the next readiness review

Vendor Evaluation Scorecard

Before a Cyprus Investment Firm can build a CySEC-ready onboarding infrastructure, it must confirm that its technology vendor can actually support the evidence standard. The scorecard below maps the questions a compliance-led procurement process should include.

Scoring: 0 = Not supported | 1 = Supported manually or partially | 2 = Supported with partial audit evidence | 3 = Fully supported with exportable audit evidence per customer

Evaluation Area	Assessment Question	Max Score	Scoring Guide
Multi-Script OCR	Does the platform process Cyrillic, Arabic, and Devanagari natively without manual override escalation?	3	0=Not supported; 1=Partial manual; 2=Native OCR, no audit export; 3=Native OCR + exportable per-customer log
Liveness Detection	What liveness method is deployed? Is it certified to an anti-spoofing standard?	3	0=No liveness; 1=Static selfie only; 2=Active liveness, no iBeta cert; 3=iBeta PAD Level 1 or 2 certified
Liveness Record Format	Does each liveness record contain a timestamp, method, outcome, anti-spoofing result, and face match score?	3	0=No record; 1=Pass/fail only; 2=Partial fields; 3=All required fields, exportable per customer
AML Screening Coverage	Which sanctions lists are queried? Is script-specific name normalisation applied per list?	3	0=Single list; 1=OFAC only; 2=OFAC + EU, no script normalisation; 3=OFAC + EU + UN + script-aware matching

Override Documentation	Is the name-match override rationale logged individually per customer with specific case-based evidence?	3	0=Not documented; 1=Generic notes; 2=Case notes, no methodology link; 3=Specific rationale + documented methodology
Annual Rescreening	Does the platform support scheduled rescreening of all customers with per-customer records?	3	0=Not supported; 1=Manual only; 2=Scheduled, no per-customer record; 3=Scheduled + per-customer exportable record
KYC File Export	Can a complete customer KYC file be exported as a single package for audit purposes?	3	0=No export; 1=Partial; 2=Multiple downloads needed; 3=Single-package export with all evidence fields
Certifications & Deployment	What certifications and deployment options are available?	3	0=None; 1=Cloud + 1 cert; 2=ISO 27001 + SOC 2; 3=ISO 27001 + SOC 2 + GDPR + on-premise option
Total	**24 points maximum**	**24**	**0-16 = significant gaps | 17-20 = partial readiness | 21-24 = audit-ready**

A vendor scoring 21 or above across all eight areas is positioned to support a CySEC-ready evidence layer. Vendors scoring below 17 will require firm-side manual processes to bridge gaps, increasing audit preparation burden.

Firms completing this evaluation can review Shufti's full capability stack and check a configuration plan before finalising procurement decisions.

Pre-Audit KYC Readiness Checklist

Use this five-category checklist to conduct a self-assessment before the next CySEC audit. Three or more gaps across any combination of categories indicate compliance exposure that CySEC's audit process is likely to identify.

Category 1: Document Verification

☐ **[CRITICAL]** Does the firm's document verification system apply ICAO-compliant Cyrillic-to-Latin transliteration for Russian passports?

☐ **[CRITICAL]** Does it process Arabic documents with script-normalised name matching, without defaulting to manual override for every MENA client?

☐ **[HIGH]** Does it handle Devanagari script from Indian and Nepali passports without manual escalation?

☐ **[HIGH]** Are OCR results and document authenticity decisions logged in customer files with timestamps?

Category 2: Sanctions and PEP Screening

☐ **[CRITICAL]** Does the AML screening system query OFAC, EU consolidated lists, and UN Security Council lists simultaneously?

☐ **[HIGH]** Are override decisions documented with specific, case-based rationale in each customer file?

☐ **[HIGH]** Are all customers rescreened on a schedule documented in the firm's AML policy, with results recorded per customer?

☐ **[MEDIUM]** Is the fuzzy matching calibration methodology documented, including the threshold approach applied per script type?

Category 3: RCOS and Liveness Detection

☐ **[CRITICAL]** Does the firm's unattended RCOS include genuine liveness detection, not just static selfie capture?

☐ **[CRITICAL]** Are liveness records timestamped and stored per customer with method, outcome, and anti-spoofing result?

☐ **[HIGH]** Is CySEC notification evidence for the firm's RCOS implementation retained in firm records?

☐ **[HIGH]** Has the RCOS risk assessment been reviewed since the December 1, 2024, implementation?

Category 4: EDD for High-Risk Client Profiles

☐ **[CRITICAL]** Do high-risk client files contain a documented sanctions-risk assessment covering nationality, beneficial ownership, source of funds, product exposure, and payment routes where relevant?

☐ **[HIGH]** Does EDD documentation include beneficial ownership identification at the 25% threshold under Cyprus AML Law 188(I)/2007?

☐ **[HIGH]** Are PEP clients identified with senior management approval documented in the file?

☐ **[MEDIUM]** Are Tier 3 and Tier 4 clients reviewed on a documented periodic cadence appropriate to their risk rating?

Category 5: Audit Trail and Record Retention

☐ **[CRITICAL]** Are all KYC records retained for at least five years post-transaction per Law 188(I)/2007?

☐ **[HIGH]** Can the compliance team produce a complete customer KYC file (identity documents, liveness records, screening logs, EDD files, annual reviews) as a single export?

☐ **[HIGH]** Do STR/SAR decision trails reference specific transaction monitoring rules, not general suspicion?

☐ **[MEDIUM]** Are customer files indexed by unique customer identifier and searchable by document type, risk rating, and nationality?

Scoring Interpretation:

0 to 2 gaps across all five categories: the firm's KYC infrastructure is substantively aligned with CySEC's current evidence expectations. 3 to 5 gaps: identifiable compliance exposure requiring prioritised remediation before the next audit cycle. Six or more gaps (particularly in Critical items): the firm's onboarding infrastructure requires material remediation.

Three or more Critical gaps?

Compliance teams can walk through how Shufti handles document verification, liveness detection, AML screening, and evidence export for CySEC-regulated workflows.

Request a Demo

CySEC KYC Evidence Pack Template

A complete customer file is not a collection of documents. It is a structured evidence pack that allows an auditor to reconstruct every onboarding and monitoring decision for a specific customer. The template below defines the required fields, the data each field should contain, and what absence creates from an audit-exposure perspective.

Compliance teams can use this template to assess if their current document management infrastructure captures all required fields per customer, and to brief their technology vendor on the exact evidence format required for CySEC audit readiness.

Evidence Field	Data Point	What Absence Creates
Customer identifier	Unique customer reference (system-generated)	Cannot link the verification record to the customer file
Document type and country	E.g. Russian Federation Passport	The auditor cannot confirm document was verified to the standard
Verification timestamp	Date and time of document check	No evidence of when verification occurred
OCR result	Extracted name, DOB, document number, expiry	Cannot demonstrate data extraction quality
Document authenticity decision	Pass / Fail / Refer + confidence score	Only binary result; no quality evidence

Liveness method	E.g. 3D liveness detection, iBeta PAD Level 2	Cannot confirm unattended RCOS meets PS-01-2024
Liveness outcome	Confirmed live / Failed / Escalated	No proof that a liveness check was run
Anti-spoofing result	Presentation attack detection: pass/ fail	Gap in the liveness evidence standard
AML screening result	Lists checked, date, match status	Cannot confirm sanctions check ran on the correct date
Override rationale (if applicable)	Case-specific reason for match decision	Override appears arbitrary (audit exposure)
EDD status	Standard CDD / Elevated / EDD triggered	Risk categorisation not evidenced in the file
Annual rescreening date	Date, lists checked, result, reviewer	No evidence of periodic sanctions refresh
Final decision and reviewer	Approved / Declined / Referred + reviewer ID	Decision trail incomplete
File export status	Exported as single audit pack: Yes / No	Cannot produce a complete file on demand

Example: Russian Passport Onboarding Workflow

The following sequence illustrates how a CySEC-ready onboarding flow handles a Russian passport, from document capture through to customer file completion:

- Customer submits a Russian passport. The system detects Cyrillic MRZ and applies ICAO Document 9303 transliteration to extract the canonical Latin-script name
- Script-specific OCR logs document type (Russian Federation Passport), country, MRZ extraction result, confidence score, and verification decision, stored timestamped in the customer file
- Name is normalised per ICAO transliteration logic and submitted to AML screening across OFAC, EU consolidated list, and UN Security Council lists simultaneously, with script-specific fuzzy matching applied
- Face verification runs with 3D liveness detection. The timestamp, method, outcome, anti-spoofing result, and face match score are logged in the customer file
- Risk-based EDD check assesses sanctions-risk indicators (nationality, residence, ownership, source of funds, product type, payment route). The assessment is documented in the EDD section of the customer file
- All fields above are exported as a single, indexed customer audit pack, retrievable by customer identifier on demand

Note: This workflow sequence illustrates what a CySEC-ready onboarding infrastructure should produce per Russian passport customer. CIFs should map this against their current vendor's output to identify evidence gaps before audit.

About Shufti Pro

Shufti is an identity verification and AML screening platform serving regulated financial services firms, including Cyprus-licensed investment firms, across more than 240 countries and territories. The platform combines document verification, face verification, AML screening, and verification workflow management in a single system designed to support compliance teams that need both operational speed and defensible, well-organised evidence.

10,000+

actively processed documents types

240+

actively processed countries and territories

150+

languages and scripts, including Cyrillic, Arabic, and Devanagari

AML screening across

3500+

watchlist sources with 15-minute update frequency

Shufti's Document Verification covers 10,000+ actively processed document types from 240+ countries, with proprietary OCR across 150+ languages. For Cyprus CIFs, the platform processes Russian passports using ICAO Document 9303 transliteration standards, Arabic identity documents using script-normalised name matching, and Indian and Nepali passports in Devanagari script without manual escalation.

The platform uses zero-shot AI, recognising new document variants without requiring manual template configuration. Document verification records include OCR output, document type, country, confidence score, decision, and timestamp per verification.

The platform uses zero-shot AI, recognising new document variants without requiring manual template configuration. Document verification records include OCR output, document type, country, confidence score, decision, and timestamp per verification.

Face Verification and Liveness Detection

Shufti's Face Verification uses 3D liveness detection, certified to iBeta PAD Level 1 and Level 2 anti-spoofing standards, with a 98.22% acceptance rate and 2.98-second average response time. Verification records include timestamp, liveness method, outcome, face match score, and anti-spoofing result: the fields required for a CySEC-ready liveness evidence pack.

AML Screening

Shufti's AML Screening queries 3500+ watchlist sources across OFAC, EU consolidated lists, UN Security Council lists, and national sanctions registers, with 20 million records updated every 15 minutes and a 2.32-second average screening response time. Override decisions are logged per customer. Rescreening can be scheduled across a customer portfolio, with per-customer records produced on each cycle.

Deployment and Certifications

Shufti operates across SaaS, Private Cloud, and On-Premise deployment models. The platform holds ISO 27001, SOC 2 Type II, and GDPR-aligned certifications. For CIFs with data residency requirements, on-premise deployment is available: a differentiator from most identity verification vendors, which offer cloud-only infrastructure.

For Cyprus Investment Firms using Shufti, the goal is not only faster onboarding. It is a defensible KYC evidence layer that supports cross-border growth while reducing manual review, sanctions-screening uncertainty, and audit-preparation burden.

Shufti

See Shufti Configured for CySEC-Regulated Onboarding

Since December 1, 2024, CySEC's RCOS requirements have been in active application. Shufti can help your team assess if current onboarding workflows produce the audit-defensible evidence required across liveness detection, document verification, AML screening, EDD, and customer-file export, ahead of the next CySEC audit cycle.

Request a Demo

shuftipro.com
sales@shuftipro.com