Shufti

Guide

Enterprise guide to remediate existing customer and business files under EU AMLR

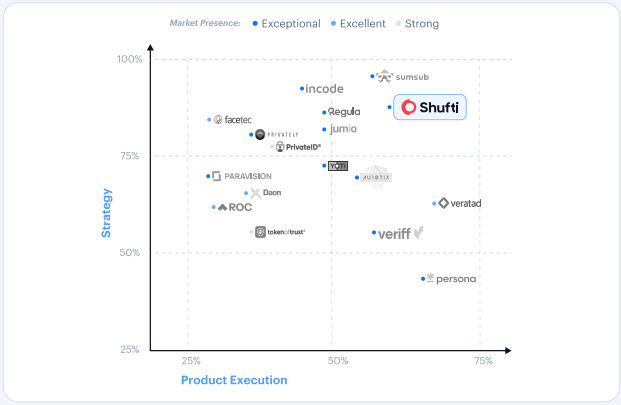
A practical guide to finding CDD gaps, prioritising existing relationships and recording decisions before the EU AMLR applies.

KJM AGE VERIFICATION | PCI DSS | iBeta L3 | ISO 27001:2022 | CE+ | QG GDPR | SOC2 | GDPR | CCPA

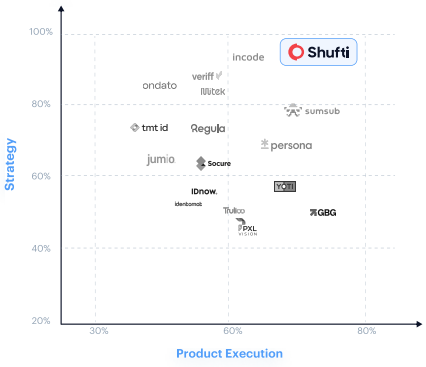
Industry Recognition 2025–2026

Recognised by leading analyst firms, government bodies and independent research organisations

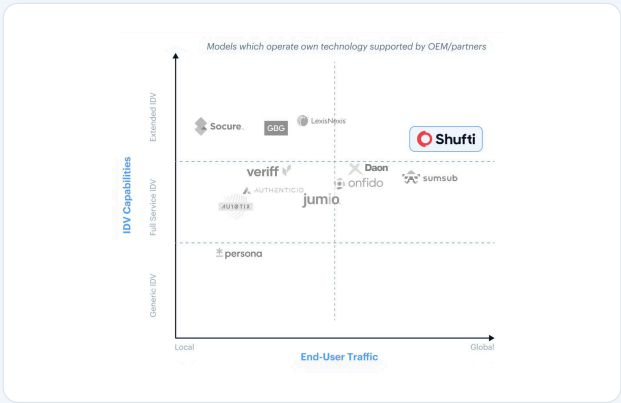
Ranked Exceptional in Liminal's 2026 Age Estimation Index



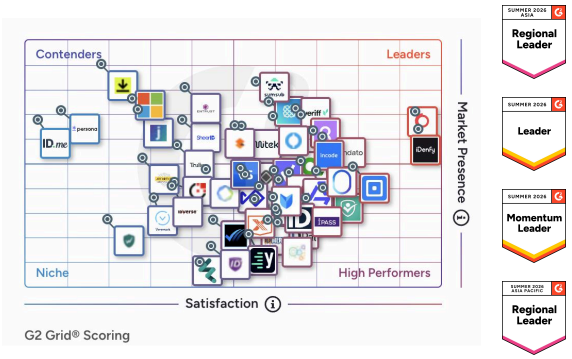
Ranked Exceptional in Liminal's 2026 Age Verification Index



Broadest global reach in the 2025 KuppingerCole Extended IDV report



Recognised as a Leader across four G2 Summer 2026 reports



Differentiated by Gartner on document diversity and country coverage

240+ Countries & Territories

10k+ Document Types

First EU company to achieve iBeta Level 3 Conformance to ISO/IEC 30107-3, with 0% APCER

iBeta Level 3 Conformance

0% APCER

Ranked Top 5 in the DHS RIVR 2025 for identity validation

0% Extraction Failure

0.67% Worst-Case FNMR

Table of Contents

How to find and remediate AMLR gaps in existing customer files

Most enterprises do not have a blank customer book. They have years of identity records, company documents, ownership charts, screening results and risk decisions, often held in different systems and created under different national rules. The problem is not always that information is absent. It is that the firm cannot quickly show whether it is still current, reliable and sufficient for the relationship that exists today.

From 10 July 2027, the EU Anti-Money Laundering Regulation (AMLR) provides a directly applicable baseline across the Union. The duties to identify customers, understand beneficial ownership, assess risk and monitor relationships all survive. What changes is the level of consistency and precision expected across the existing book.

The required response is not a one-day refresh of every old file. It is a controlled remediation program. It defines what a complete file must show, compares the existing businesses and customers against that standard, moves the riskiest or most uncertain cases first, updates only what needs work, and keeps enough evidence to reconstruct the final decision.

1. AMLR requires targeted updates to existing files

Many underlying duties already existed under the Fourth Anti-Money Laundering Directive. AMLR does not make every legacy file defective. It does, however, change several thresholds, definitions, data requirements and review rules that firms can test directly across the existing book.

The comparison below includes only changes that can require an existing customer file to be reopened, updated or reassessed. The pre-AMLR column describes the EU baseline under Directive (EU) 2015/849; national rules may already have been stricter or more detailed.

Six AMLR changes can require existing files to be reopened or updated

Customer-file update intervals

BEFORE AMLR: EU BASELINE

No EU rule said how often files must be refreshed. Ireland's law, for example, asked firms to monitor as far as risk warranted, and set no deadline at all.

FROM 10 JULY 2027

Now there is a deadline everywhere. Article 26 caps the gap between updates at one year where enhanced due diligence under Section 4 applies, and five years in every other case. Risk can shorten either, never stretch them.

EXISTING-BOOK REMEDIATION CHECK

Find files already beyond, or approaching, the relevant maximum. Do not treat one or five years as the default for every customer.

Reviews before the scheduled date

BEFORE AMLR: EU BASELINE

Files were reviewed when something known changed, such as a customer's circumstances. Germany's law worked the same way. Learning a new fact was not a written trigger on its own.

FROM 10 JULY 2027

AMLR retains those cases and expressly adds a third trigger: the firm becomes aware of a relevant fact concerning the customer.

EXISTING-BOOK REMEDIATION CHECK

Make sure new facts, monitoring findings and verified changes can reopen a file instead of waiting for the next scheduled review.

Individual identification data

BEFORE AMLR: EU BASELINE

Every Member State wrote its own list of personal details. Germany's GwG, for example, asked for name, place and date of birth, nationality and residential address, and never asked for a tax number.

FROM 10 JULY 2027

Article 22 fixes the dataset. All names and surnames, place and full date of birth, nationality or statelessness and status information, residential address and country of residence, identity document number, and any unique personal identification number.

EXISTING-BOOK REMEDIATION CHECK

Map legacy individual files against the Article 22 fields. Collect only information that is missing, outdated, doubtful or required for the current risk.

Business identification data

BEFORE AMLR: EU BASELINE

National lists diverged here too. Firms typically evidenced legal form, name and registered office under Directive (EU) 2015/849. No EU wide rule required a legal entity identifier or the disclosure of nominee shareholders and directors.

FROM 10 JULY 2027

For standard CDD, Article 22 specifies legal form and name; registered or official office; principal place of business and country of creation; legal representatives; available registration, tax and LEI identifiers; and the names and status of nominee shareholders or directors.

EXISTING-BOOK REMEDIATION CHECK

Flag files that cannot evidence the entity's current legal form, locations, representatives, identifiers or nominee roles.

Beneficial ownership threshold and calculation

BEFORE AMLR: EU BASELINE

The EU indicator was 25% plus one share or an ownership interest of more than 25%. Indirect ownership was recognised, but calculation practice could differ.

FROM 10 JULY 2027

Article 52 uses 25% or more of shares, voting rights or other ownership interest. Indirect interests are multiplied down each chain and the results from different chains are added; every ownership level is considered.

EXISTING-BOOK REMEDIATION CHECK

Rerun structures involving exactly 25% and layered holdings. Test control by other means separately; ownership percentage is not the only route to beneficial ownership.

PEP functions and family members

BEFORE AMLR: EU BASELINE

The EU minimum covered senior national functions. PEP family members were spouses or equivalent partners, children and their partners, and parents; siblings were not included.

FROM 10 JULY 2027

AMLR expressly includes heads of regional and local authorities, municipal groupings and metropolitan regions with at least 50,000 inhabitants. It also adds siblings as family members, but only for heads of State or government, ministers, deputy or assistant ministers, and equivalent EU or third-country functions.

EXISTING-BOOK REMEDIATION CHECK

Extend role and relationship screening, but do not label every PEP's sibling a family member. Apply the sibling rule to the functions named in AMLR, then check national implementation. Member States may widen the sibling definition where their social and cultural structures and risk profile justify it.

LEGAL STATUS

Final law: AMLR applies from 10 July 2027 and Article 26 sets the ongoing-monitoring, update and event-review framework. Draft detail: AMLA's Article 28(1) CDD RTS and Article 26(5) guidelines are past consultation and unadopted as at [date]. Firm decision: prioritisation, outreach, escalation, quality assurance and case ownership remain part of each firm's operating model.

The draft CDD RTS proposes that information on customers already in a business relationship be brought into line on a risk-sensitive basis within the Article 26 periods, with those periods starting when the future delegated regulation applies. It is a planning assumption from a February 2026 draft, not a statutory deadline. Firms should prepare the inventory and process now.

Article 26 therefore makes file maintenance a continuing cycle of monitoring, scheduled updates, event-triggered reviews and targeted-financial-sanctions verification.

2. A remediated file must show who the customer is, the current risk and why the relationship can continue

A firm cannot find gaps until it defines the file it wants to finish with. The target is not a folder full of documents. It is a record that connects verified facts to the current risk decision.

For an individual, the file should establish identity, relevant residence information, the purpose of the relationship, expected activity, screening results and current risk. For a business, the same logic applies, but the file must also explain the legal entity, authorised representatives, ownership and control. Business remediation is usually heavier because a current certificate of incorporation does not, by itself, show who ultimately owns or controls the customer.

The file must show	Individual customer	Business customer
Identity	Names, date and place of birth, nationality and residence or contact information, with suitable verification evidence.	Legal name, form, registration and tax identifiers where available, registered office, principal place of business and country of creation.
People connected to the relationship	Any authorised person or other person on whose behalf or for whose benefit activity is conducted.	Legal representatives, authorised persons, directors where relevant, beneficial owners and anyone exercising control by other means.
Purpose and expected activity	Why the relationship exists, expected use and activity, and occupation where relevant.	Business activity, economic rationale, expected products, activity and flows, with source and destination of funds where necessary.
Risk and screening	Current risk assessment, PEP status, targeted financial-sanctions checks and other screening required by policy.	Entity and connected-party risk, ownership complexity, geography, PEP and targeted financial-sanctions exposure, plus relevant screening.
Decision evidence	Reason for review, information used, reviewer, outcome and next review point.	Ownership rationale, verification sources, unresolved issues, approvals, outcome and next review point.

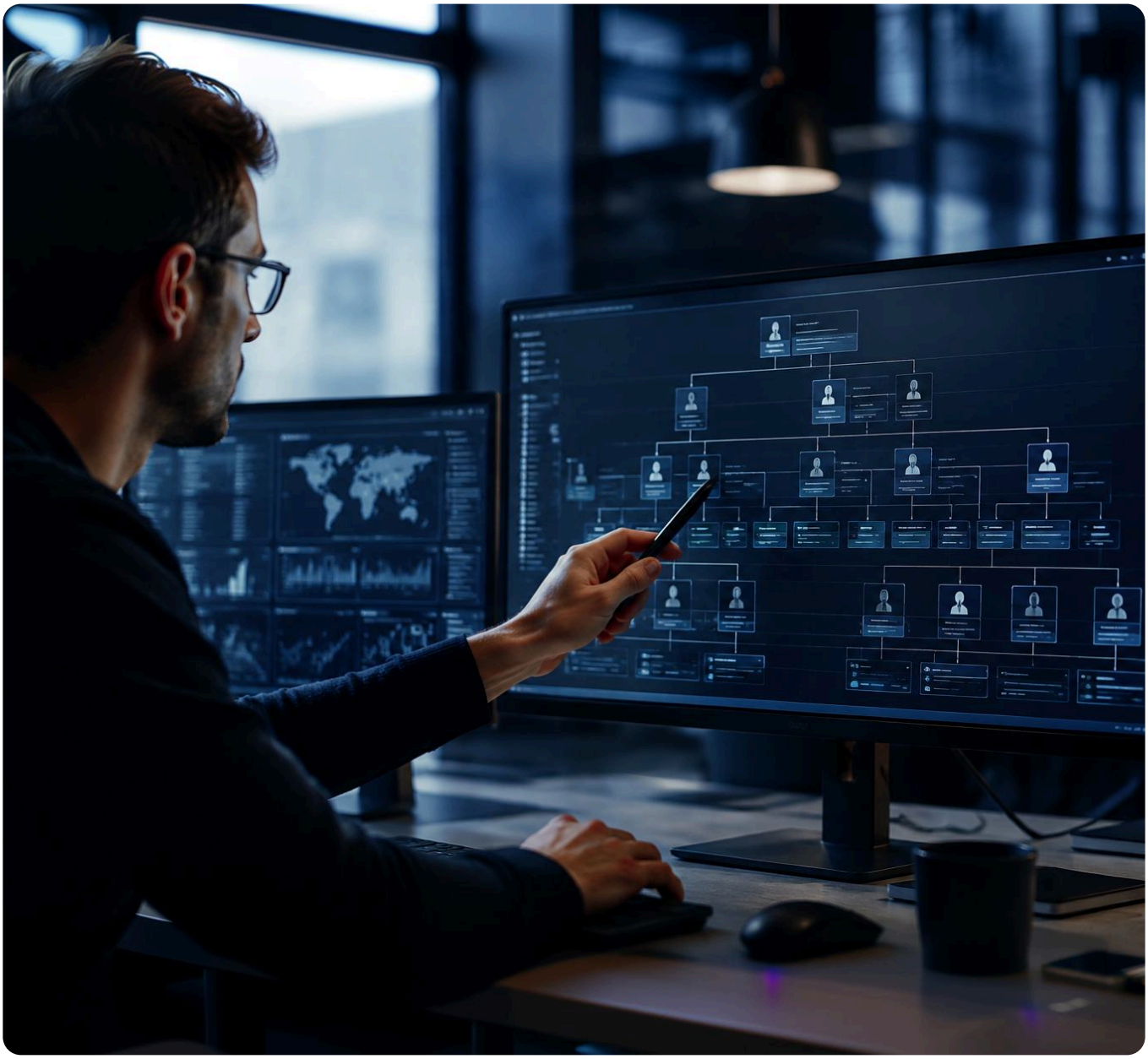
Source note: Regulation (EU) 2024/1624, Articles 20, 22, 25 and 26.

For business customers, registration evidence alone does not establish current ownership and control

For a business customer, use current register information to establish legal existence and support the ownership review. Then test whether the recorded ownership and control picture is complete, plausible and consistent with other evidence. If the beneficial owner cannot be identified after all possible means have been exhausted, AMLR requires that outcome and the steps taken be recorded; the senior-managing-official route is not a shortcut around an incomplete ownership assessment.

Every business file does reach a point where its ownership information is rechecked, either on its review cycle or sooner if an event pulls it forward. What that recheck means varies, and it rarely means rebuild. Where the owners on file still match the registers and nothing signals a change, confirm and record. Reconstruction is reserved for structures that are old, incomplete or contradicted. One detail does catch older files. The threshold is now 25% or more, where the pre-AMLR baseline said more than 25%, so a holder sitting at exactly 25% counts today and may be absent from a file built under the old wording. At minimum, each business review re-runs that threshold test and the separate control-by-other-means check.

The completion test is simple: could another trained reviewer open the file and understand what was checked, what changed, how risk was assessed, who made the decision and when the relationship must next be reviewed? If not, the file is not finished.



AMLR REMEDIATION

Turn existing customer data into remediation-ready evidence

AMLR remediation depends on more than collecting documents. Firms need reliable identity, business, ownership and screening evidence that can support consistent risk decisions.

Shufti helps organisations verify customers, businesses and connected parties while creating traceable evidence that compliance teams can review, reuse and monitor throughout the customer lifecycle.

SEE HOW SHUFTI SUPPORTS AMLR REMEDIATION WORKFLOWS →

3. Assess existing files before asking customers for new information

Starting with outreach creates unnecessary friction and usually produces a poor estimate of the work. Start with the book. Bring together enough information to assess each relationship: customer type, current risk level, last completed review, available identity or entity evidence, ownership information, screening status, known trigger events, open alerts and unresolved exceptions.

Then compare each file with the target standard. The review should distinguish a real information gap from a storage or retrieval problem. A reliable fact already held by the firm may still be usable. A document may be present but no longer prove the current position. A record may be current yet lack the reasoning that connects it to the risk decision.

Assign each file one outcome: current, reuse, update, investigate or escalate

Outcome	What it means	Next action
1. Current	Information and evidence remain sufficient for the present risk.	Confirm the review and retain the record.
2. Confirm or reuse	Reliable information exists, but its current relevance must be checked.	Confirm through internal or reliable independent sources.
3. Update	A defined field, document or screening result is outdated.	Refresh only the affected information.
4. Investigate	Material evidence is missing, inconsistent or cannot be validated.	Obtain further evidence and resolve the conflict.
5. Escalate	Risk has increased, CDD cannot be completed or the case may require EDD, restriction, exit or reporting consideration.	Route to the authorised decision-maker.

The first outcome is the one that keeps the exercise honest, and files earn it by comparison, not by assumption. For individuals the comparison is concrete, because AMLR fixes the data set. A complete file holds all names and surnames, place and full date of birth, nationality and specified status information, a national ID where applicable, usual residence or contact address and a tax ID where available, plus verification evidence that still meets the standard, purpose, expected activity, current screening results and a risk rating with written reasoning. Where every field is present, supported and undisturbed by doubt, the file takes outcome 1, Current, and the customer never hears from you. Files missing fields, common wherever onboarding ran under an older national regime, take outcome 3, Update, and join the queue.

Prioritise triggered, higher-risk and uncertain files before routine updates

A large book needs a living queue, not one fixed campaign list. Priority should increase where a trigger event has occurred, the customer is higher risk, the gap is material, the evidence is old or unreliable, ownership or control has changed, sanctions exposure may exist, activity no longer fits the profile, or the next required review is approaching.

PRACTICAL RULE

Do not contact every customer. Contact the customer when the required information cannot be confirmed, reused or obtained from an appropriate source, or when the firm needs the customer to explain a change or inconsistency.

4. Use one controlled process to remediate both individual and business files

The individual and business paths contain different evidence, but they should not become two different operating models. One process makes ownership, escalation and quality assurance easier to control.

01 **Open the case and record why it exists.** Use a specific reason: scheduled review, trigger event, missing-data assessment, monitoring alert, sanctions or PEP development, or a quality finding.

02 **Identify the exact gap.** State whether the problem concerns identity, legal existence, authority, ownership, purpose, expected activity, screening, risk or completion evidence.

03 **Check what can be confirmed or reused.** Review internal records, recent checks, official registers and other suitable sources before asking the customer for information already available.

04 **Collect only what is missing, outdated or doubtful.** Make the request specific. Explain what is needed, why it is needed and the response route. Keep a record of each attempt.

05 **Verify the relevant people and entity.** For an individual, confirm identity and relevant personal information. For a business, verify legal existence, authority, ownership, control and beneficial owners.

06 **Refresh screening and reassess risk.** Consider PEP status, targeted financial sanctions, adverse information and other required screening, then compare expected activity with what the firm has observed.

07 **Make the relationship decision.** Confirm or update the file, apply EDD, obtain senior approval, restrict activity where appropriate, escalate for exit, or consider suspicion under the firm's reporting process.

08 **Record the outcome and return the file to monitoring.** Store the evidence, reasoning, approvals, completion date and next review point. Close the case only when the decision can be reconstructed.

Customer non-response requires documented outreach, risk review and escalation

Non-response is not a decision by itself. Record the attempts, check whether suitable information can be obtained elsewhere, consider the customer's risk and the materiality of the missing information, and follow the firm's escalation rules. Where the missing information prevents completion of the CDD measures in Article 20(1), Article 21 requires the obliged entity to refrain from carrying out a transaction or establishing a new relationship; for an existing relationship, it must terminate it and consider whether suspicion should be reported, subject to the Regulation's specific exceptions and alternatives. Technology should not decide that outcome.

Conflicting evidence must be resolved or escalated before the file is closed

Do not average two inconsistent answers into a clean field. Identify the conflict, obtain a more reliable source or explanation, determine whether the difference changes identity, authority, ownership, purpose or risk, and record how it was resolved. A difference between the firm's beneficial-ownership information and the central register must be handled under Article 24's discrepancy process, including its limited correction route for specified minor or outdated entries.

Worked example: an ownership change requires UBO verification, re-screening and a new risk decision

Northbridge ICT is a hypothetical medium-risk business customer. Monitoring identifies a registry update: a new shareholder now holds 30% and one previous director has left. The customer file still shows the old ownership chart and the departing director as an authorised representative.

01 Open an event-driven review and record the registry change as the trigger.

02 Obtain current entity and representation information and reconstruct the ownership chain.

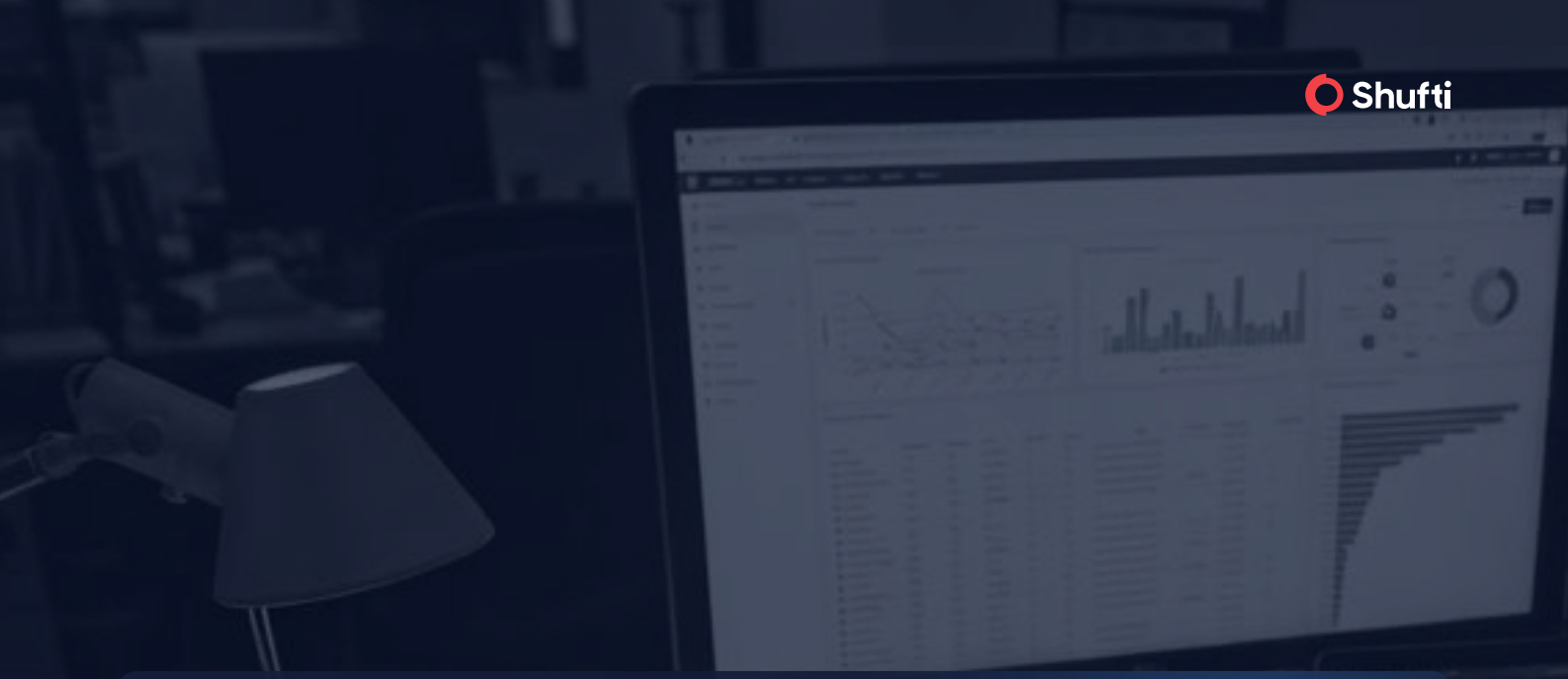
03 Identify and verify the new beneficial owner and confirm who is authorised to act.

04 Screen the entity, new beneficial owner and relevant connected parties; resolve any matches.

05 Compare the revised ownership, geography and expected activity with the existing risk assessment.

06 Record the reviewer's decision, any approval, the updated risk rating and the next review date.

If the new owner is verified, no material adverse information is found and the activity still matches the relationship, the firm may update the file and continue. If ownership remains unclear or the change creates higher risk, the case moves to enhanced review or escalation. The trigger starts the review; it does not predetermine the outcome.



AMLR READINESS

Scale remediation without losing control

Customer file | Verification | Screening | Risk review | Ongoing monitoring

A successful AMLR programme requires more than individual checks. Firms need a repeatable process that connects verification, screening, monitoring and decision evidence across their existing customer base.

Shufti provides verification and screening capabilities that help compliance teams strengthen remediation workflows while keeping final risk decisions under their control.

EXPLORE AMLR READINESS WITH SHUFTI →

5. Remediation is complete only when another reviewer can reconstruct the decision

Completion is not the date on which the last document arrived. It is the point at which current evidence supports a current decision and the record explains how that decision was reached.

The closure record should show why the review began; what the firm already held; what was missing, outdated or inconsistent; which information was confirmed, reused or collected; which verification and screening checks were performed; how the risk view changed; who decided and approved the outcome; and when the relationship will next be reviewed.

Once closed, the file returns to periodic review, event-trigger monitoring, transaction or activity monitoring where applicable, PEP and sanctions screening, exception management and quality assurance. Remediation clears a known gap. Ongoing monitoring is what stops the file becoming stale again.

6. A scalable remediation programme needs clear ownership, completion rules and quality control

A good pilot can still fail at scale if the firm has not decided who owns the queue, who can approve higher-risk outcomes, what non-response means, or what evidence closes a case. Before large-scale outreach, establish the customer-file standard, one inventory of existing relationships, trigger and prioritisation rules, named case owners, decision rights, escalation routes, completion criteria, quality assurance and management reporting.

Test the process on representative files: a straightforward individual, an expired document, a higher-risk customer, a business with layered ownership, a non-responsive customer and a case with conflicting evidence. The test should reveal whether data can be retrieved, whether checks can be reused, where hand-offs stall and whether another reviewer can reconstruct the final decision.

Shufti supplies verification and screening evidence; the obliged entity makes the risk and relationship decision

Activity	Shufti can support	The obliged entity remains responsible for
Identity refresh	Document, biometric, NFC and electronic identity checks, configured for the required journey.	Deciding when re-verification is necessary and whether the evidence is sufficient for the risk.
Business remediation	Entity verification, director and beneficial-owner identification, ownership mapping and connected-party checks.	Understanding ownership and control, resolving discrepancies and deciding whether the relationship is acceptable.
Screening	PEP, sanctions, watchlist and adverse-media screening for individuals, entities and relevant connected parties.	Reviewing potential matches, assessing relevance and deciding how findings affect risk.
Ongoing controls	Continuous screening and monitoring signals that can identify changes after onboarding.	Defining triggers, thresholds, investigation standards and escalation routes.
Evidence	Verification results, screening outputs and traceable records from the checks performed.	Maintaining the complete CDD record, reasoning, approvals and retention controls.
Final outcome	Decision-support information and workflow inputs.	Assigning the risk profile and deciding to approve, restrict, report, continue or exit. These decisions cannot be outsourced.

Source note: AMLR keeps the obliged entity liable for outsourced tasks and prohibits outsourcing specified decisions, including the customer risk profile, entry into a relationship and suspicious-activity reporting.

Shufti can clear a large share of that queue in bulk before anyone contacts a customer. You can re-screen an existing book against PEP, sanctions, watchlist and adverse-media data, monitor it for status changes, and refresh business and beneficial-owner information from registry sources where coverage allows, with results returned per customer and evidence attached. One pass like that surfaces stale screening, new matches and ownership that no longer matches the file. Identity re-verification still needs the customer to complete a check, one more reason to reserve outreach for files nothing else can close. And no provider can see inside a firm's own records, so the field-by-field comparison from Section 3 runs on the firm's systems, with the bulk results feeding it as the freshest evidence. The firm builds the list. Shufti fills in what the world outside its records says about each file.

The useful question is therefore not whether technology can ‘make the firm AMLR-compliant’. It cannot. The question is whether the operating model can use verification, registry, screening and monitoring outputs to reach consistent human decisions across the existing book, and show the evidence later.

Primary AMLR sources and legal-status limits for this guide

This guide explains a practical operating approach. It does not replace legal advice. Firms should test the final Regulation and adopted AMLA instruments against their own activities, risk assessment, customer base and applicable national supervisory expectations.

01 **Regulation (EU) 2024/1624 (AMLR)** — Final law; especially Articles 20–26 and 90.

02 **Directive (EU) 2015/849, consolidated text** — Pre-AMLR CDD and existing-customer baseline; especially Articles 13–14.

03 **AMLA consultation on the draft CDD RTS under Article 28(1)** — Consultation closed 8 May 2026; instrument remains draft as at 09 Sep 2026.

04 **AMLA consultation on draft ongoing-monitoring guidelines under Article 26(5)** — Consultation closed on 3 September 2026; not adopted as at 09 Sep 2026.

05 **Shufti identity verification** — Current product capability reference.

06 **Shufti business verification** — Current entity, ownership and UBO capability reference.

07 **Shufti ongoing monitoring** — Current monitoring capability reference.

STATUS CONTROL

Every statement drawn from AMLA's February or June 2026 consultation material is treated as draft. The guide should be reviewed when the CDD RTS or Article 26(5) guidelines are adopted or materially revised.

Shufti

Prepare your existing customer book for AMLR

AMLR readiness starts with understanding where your current customer files stand. Work with Shufti to identify evidence gaps, review remediation workflows and understand where identity verification, business verification, screening and monitoring capabilities can support your compliance operations.

Request a Demo

Shufti is based in the United Kingdom and operates offices worldwide.

United States
16200 SW Pacific Hwy, Suite H PMB 1053, Tigard, OR

Cyprus
Arch. Makarios III Avenue 229, Limassol

Dubai
Unit 507, Level 5, Gate District Precinct Building 03, DIFC, Dubai

Hong Kong
8 Queen's Road East, Wan Chai, Hong Kong

Pakistan
322-G3 Main Blvd, Johar Town, Lahore, Pakistan

Singapore
68 Circular Road #02-01, Singapore

United Kingdom
Office 408, Coppergate House, 10 Whites Row, London E1 7NF

shuftipro.com
sales@shuftipro.com