Shufti

The AMLR readiness checklist

Every control from the online checklist, in one printable workbook. Mark where your programme stands, then work the gaps.

87 CONTROLS
TWELVE WORKSTREAMS

INSTRUMENT	APPLIES FROM	LAST REVIEWED
Regulation (EU) 2024/1624	10 July 2027	13 August 2026

COMPANION TO THE AMLR READINESS CHECKLIST AT SHUFTIPRO.COM

HOW TO USE IT FOUR MARKS, TWELVE WORKSTREAMS

A readiness map, not a grade

Work through the 87 controls and mark each one. Score at the end. The result is a prioritisation of what to build before 10 July 2027, not a pass mark.

☐

IN PLACE

1 POINT

Implemented, documented, and testable today.

☐

IN PROGRESS

½ POINT

Started, or in place but incomplete, undocumented, or inconsistent across markets.

☐

NOT STARTED

0 POINTS

No work done. Every gap here needs an owner and a date.

☐

N / A

EXCLUDED

Does not apply to you. N/A items leave the denominator, so marking one raises your score.

READING THE TAGS

CRITICAL PATH Long lead time, or blocks work downstream. Start these first. 22 of the 87 controls carry it.

ART. 11(1) The provision the control comes from. A bare article number is Regulation (EU) 2024/1624; anything else is named.

GOOD PRACTICE Recommended, and not a requirement of the Regulation.

GROUPS ONLY Applies only if you are part of a group. A standalone entity can mark these N/A.

CRYPTO-ASSET SERVICE PROVIDERS Applies only to that type of obliged entity. Mark N/A if it is not you.

FROM 10 JUL 2029 A date other than 10 July 2027 governs the control.

Before you start

Set your obliged-entity type first, then mark every control outside it N/A rather than skipping it, so the score stays honest. Article references are to the Official Journal text. AMLA's regulatory technical standards were still being issued as of August 2026, so procedural detail may tighten before it applies.

The aim

Not a perfect score today. A clear map of what to fix, in what order, before 10 July 2027.

CONTENTS 87 CONTROLS

Twelve workstreams

01	Scope and applicability	6 CONTROLS	05
02	Governance, policies and controls	8 CONTROLS	06
03	Business-wide risk assessment	6 CONTROLS	07
04	Customer due diligence	12 CONTROLS	08
05	Beneficial ownership	9 CONTROLS	11
06	Enhanced due diligence and high-risk cases	7 CONTROLS	12
07	Sanctions and targeted financial measures	5 CONTROLS	14
08	Monitoring, reporting and FIU cooperation	8 CONTROLS	15
09	Records, retention and data protection	5 CONTROLS	16
10	Outsourcing, reliance and third parties	5 CONTROLS	17
11	Sectoral limits and specific obligations	10 CONTROLS	18
12	Technology, data and operating model	6 CONTROLS	20

Who is an obliged entity

Fourteen of the 87 controls apply only to particular obliged-entity types. Confirm which of these you are, then mark the rest N/A.

CREDIT & FINANCIAL INSTITUTIONS

Credit and financial institutions are obliged entities for the whole of their business.

CRYPTO-ASSET SERVICE PROVIDERS

Crypto-asset service providers are obliged entities for the whole of their business. MiCA defines what a crypto-asset service provider is and who may operate as one; AMLR and the Transfer of Funds Regulation carry the AML duties.

TCSPS, LEGAL & ACCOUNTING

Trust or company service providers are covered for their whole business. Lawyers, notaries and other independent legal professionals, auditors, external accountants and tax advisers are obliged entities only for defined activities and transactions, so test the activity before applying a control.

REAL ESTATE

Estate agents and other real-estate professionals are covered on an activity-dependent basis. Both parties to the transaction count as customers, which doubles the due-diligence population on every deal.

GAMBLING

Providers of gambling services are obliged entities, and Member States may exempt defined low-risk gambling services under Article 4. Confirm the national position before scoping.

HIGH-VALUE GOODS TRADERS

Traders in high-value goods are obliged entities above defined thresholds, so scope depends on the product line and the transaction size rather than on the business as a whole.

PROFESSIONAL FOOTBALL

Professional football clubs are obliged entities from 10 July 2029, and only for four transaction types: with an investor, with a sponsor, with football agents or other intermediaries, and for the purpose of a player's transfer. Member States may exempt clubs entirely or partly under Article 5. Football agents are covered more broadly. Treat the controls below as the superset and scope them to those transactions.

01 Scope and applicability

6 CONTROLS

Before anything else, pin down which of your entities, products and jurisdictions the regulation captures, and from when.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Map every legal entity, branch and product against the AMLR list of obliged entities AMLR applies directly, so group entities in different Member States can no longer sit under different national scopes. Produce a single entity-by-entity determination and keep the reasoning. CRITICAL PATH · ART. 3	☐	☐	☐	☐
Confirm whether newly captured activities pull you into scope The obliged-entity list expands to cover crypto-asset service providers, crowdfunding service providers and intermediaries, and traders in high-value goods above defined thresholds. Businesses that were out of scope under national law may now be in. CRITICAL PATH · ART. 3	☐	☐	☐	☐
Check for national gold-plating that survives alongside AMLR AMLD6 still leaves Member States room to extend scope to further sectors. Confirm for each country you operate in whether local law adds obliged entities or obligations on top of the regulation. AMLD6	☐	☐	☐	☐
Align AMLR obligations with your MiCA and Transfer of Funds Regulation programme Crypto-asset service providers are brought fully into the AML perimeter in line with MiCA. Treat AMLR, MiCA authorisation and travel-rule obligations as one build, not three. CRITICAL PATH · ART. 3 · CRYPTO-ASSET SERVICE PROVIDERS	☐	☐	☐	☐
Plan for the 2029 start date for professional football Obligations for professional football clubs and football agents apply from 10 July 2029 rather than 2027. Build the runway now, but scope the programme to that date. ART. 3 · FROM 10 JUL 2029 · PROFESSIONAL FOOTBALL	☐	☐	☐	☐
Set a single group-level AMLR programme owner and budget line Fragmented, country-by-country remediation is the most common way firms miss the date. One accountable owner, one plan, one reporting line to the board. GOOD PRACTICE · GROUPS ONLY	☐	☐	☐	☐

02 Governance, policies and controls

8 CONTROLS

AMLR moves AML governance up the org chart and puts approval rights in named hands (Articles 9–11).

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Designate a compliance manager from within the management body AMLR requires one member of the management body in its management function to be responsible for compliance with the Regulation. This is a board-level designation, not a functional one. Where size and complexity justify it, one person may hold both this and the compliance officer role, and a one-person business performs both itself under Article 11(7), and the person carries responsibility for ensuring policies are consistent with risk exposure and are actually implemented. CRITICAL PATH · ART. 11(1)	☐	☐	☐	☐
Appoint a compliance officer to run AML/CFT day to day The compliance officer is appointed by the management body, must hold sufficiently high hierarchical standing, is responsible for policies and controls in day-to-day operation including targeted financial sanctions, and is the contact point for competent authorities. If your MLRO currently reports three levels down, that structure needs changing. CRITICAL PATH · ART. 11(2)	☐	☐	☐	☐
Rewrite internal policies for management-body approval Internal policies must be approved by the management body in its management function. Procedures and controls must be approved at least at compliance-manager level. Record the approval, the date and the version. CRITICAL PATH · ART. 9	☐	☐	☐	☐
Cover every mandated topic in the policy set Policies and procedures must address the business-wide risk assessment, risk management, customer due diligence, suspicious activity reporting, outsourcing, reliance on third parties, record retention and personal data processing. Gap-check your current suite against that list. ART. 9	☐	☐	☐	☐
Build group-wide policies and a mechanism to apply them across the group Group-wide requirements cover parent undertakings, subsidiaries and branches, including those in third countries, with additional measures where third-country law prevents full application. ART. 16 · GROUPS ONLY	☐	☐	☐	☐

02 Governance, policies and controls CONTINUED

8 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A

Refresh the AML training programme and evidence completion

Training must be tied to the roles staff actually perform and to the risks identified in the business-wide risk assessment. Attendance records and comprehension testing are what supervisors ask for.

ART. 12

Run fit-and-proper and integrity checks on relevant staff

Article 13 is headed "Integrity of employees" and makes screening of staff in roles exposed to money laundering and terrorist financing risk an explicit control, not an HR nicety. Define which roles are in scope and how often checks repeat.

ART. 13

Set board-level MI so the management body can actually discharge its role

If the management body approves the policies, it needs reporting good enough to challenge them: alert volumes, backlog age, SAR conversion, CDD refresh coverage, and open supervisory findings.

ART. 9-11

03 Business-wide risk assessment

6 CONTROLS

The risk assessment is the document every other control is measured against. It has to be evidenced, current, and owned.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A

Produce a documented business-wide risk assessment under AMLR

The business-wide risk assessment is the anchor for internal controls, training and the risk-based application of CDD. It must be a standing, evidenced document, not a slide deck refreshed after an audit.

CRITICAL PATH ART. 10

Cover customers, products, services, transactions, delivery channels and geographies

Each risk factor category needs its own assessment and rationale. Where you rate a category low, say why, with data.

ART. 10

03 Business-wide risk assessment CONTINUED

6 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Feed in the supranational and national risk assessments The Commission's supranational assessment and each relevant national risk assessment are inputs you are expected to have considered and reconciled against your own findings. ART. 10, AMLD6	☐	☐	☐	☐
Define a review trigger and cadence Set both a fixed refresh cycle and event triggers: new product, new market, new delivery channel, material incident, supervisory finding. ART. 10	☐	☐	☐	☐
Trace each control back to a risk in the assessment Supervisors increasingly test the linkage rather than the document. Every control should be attributable to an identified risk, and every material risk should have a named control. ART. 9-10	☐	☐	☐	☐
Assess residual risk and get it formally accepted Record what risk remains after controls, who accepted it and at what level. Unaccepted residual risk is a finding waiting to happen. ART. 10	☐	☐	☐	☐

04 Customer due diligence

12 CONTROLS

CDD is now written as a single harmonised rulebook rather than 27 national interpretations. Expect your existing procedures to need rewriting, not just retitling.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Rebuild CDD procedures against the harmonised rulebook AMLR replaces divergent national CDD interpretations with one set of rules applying identically across the EU. Assume your national-flavoured procedures need rewriting rather than remapping. CRITICAL PATH CH. III	☐	☐	☐	☐
Confirm identification and verification data points for natural persons Check the specific attributes AMLR requires you to collect and verify, and confirm your onboarding forms and vendor configuration capture all of them for every market. CRITICAL PATH ART. 22(1)(A)	☐	☐	☐	☐

04 Customer due diligence CONTINUED

12 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Confirm identification and verification for legal entities and arrangements Legal form, registration data, constitutional documents, and the persons authorised to act, with verification, not just collection. ART. 22	☐	☐	☐	☐
Define when CDD is triggered, including occasional transactions and linked operations Establish trigger events, applicable thresholds and, critically, how you detect operations that are individually below a threshold but linked. ART. 19	☐	☐	☐	☐
Support electronic identification and qualified trust services in your CDD flow AMLR contemplates identification using eIDAS-notified electronic identification means and relevant qualified trust services. If you operate in the EU, plan for EUDI Wallet acceptance rather than retrofitting it later. ART. 22(6)	☐	☐	☐	☐
Set risk-based ongoing due diligence and refresh cycles Periodic review frequency must follow customer risk, and event-driven review must be triggered by material changes. Document the model and evidence that refreshes actually happen on time. ART. 26(1)	☐	☐	☐	☐
Define your position on anonymous and non-face-to-face relationships Remote onboarding remains permitted but has to be controlled. Record how liveness, document authentication and fraud signals compensate for the absence of physical presence. ART. 22(6)	☐	☐	☐	☐

04 Customer due diligence CONTINUED

12 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A

Write the customer-acceptance and exit playbook

Where CDD cannot be completed, the relationship must not be established or must be terminated, and you must consider whether to report. Make that path unambiguous for front-line staff.

ART. 21

Remediate the back book

Existing customers onboarded under old national standards will need to be brought up to AMLR standard on a risk-based schedule. Size this early. For most firms it is the single biggest workload item.

CRITICAL PATH ART. 26(2)

Capture the legal-entity data points older KYB models tend to miss

Article 22(1)(b) requires the registered or official office and, if different, the principal place of business and country of creation; the Legal Entity Identifier where available; and the names of persons holding shares or a directorship in nominee form, including their status as nominee shareholders or directors.

ART. 22(1)(B)

Cap deferred verification at 60 days with interim controls in the meantime

Where verification is postponed for a qualifying lower-risk relationship, it must complete no later than 60 days of the relationship being established, and interim risk-management procedures such as limits on the amount, number or type of transactions apply until it does.

ART. 33(1)(A)

Treat both parties to a property transaction as customers

For estate agents and other real-estate professionals, AMLR treats both parties to the transaction as customers. That doubles the due-diligence population on every deal, and it is the most common scoping error in the sector.

CRITICAL PATH ART. 19(6)(C) REAL ESTATE

05 Beneficial ownership

9 CONTROLS

The definition tightens, the evidence burden rises, and register data alone no longer discharges the obligation.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Reconfigure UBO detection for the “25% or more” threshold The ownership test moves from “more than 25%” to “25% or more”. It sounds trivial; it changes the population. Confirm your systems and vendors use the inclusive test, and re-run the back book against it. CRITICAL PATH · ART. 51-52	☐	☐	☐	☐
Handle control through means other than shareholding Beneficial ownership through control, whether voting rights, veto rights, agreements or nominee arrangements, has to be assessed alongside ownership interest, not instead of it. ART. 51-53	☐	☐	☐	☐
Unwind multi-layer and cross-border ownership chains Indirect ownership must be calculated through the whole chain, including entities registered outside the EU. Decide how deep you go and where you stop, and document the rule. ART. 51-53	☐	☐	☐	☐
Stop treating register data as sufficient verification You must take adequate steps to verify beneficial ownership. A register extract is a starting point and a discrepancy check. It does not discharge the obligation on its own. ART. 22	☐	☐	☐	☐
Operationalise discrepancy reporting to beneficial ownership registers Where your findings differ from register data, AMLR puts the reporting duty on you as an obliged entity: without undue delay, and in any case within 14 calendar days of detection. The registers are AMLD6 machinery, but the obligation to report is not. Build the workflow, the SLA and the audit trail against that 14-day clock. ART. 24	☐	☐	☐	☐
Document the senior-managing-official fallback properly Where no beneficial owner can be identified after exhausting all means, the senior managing official may be recorded, but only with a written record of the steps taken. Blanket use of this fallback is a red flag to supervisors. ART. 51-53	☐	☐	☐	☐

05 Beneficial ownership CONTINUED

9 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Apply the tighter treatment for trusts and similar legal arrangements Settlor, trustee, protector, beneficiaries and any other person exercising ultimate control each have to be identified and recorded. ART. 58-60 · TCSPS, LEGAL & ACCOUNTING · REAL ESTATE	☐	☐	☐	☐
Handle chains where ownership and control coexist at different layers Where a multi-layered structure has ownership interest and control coexisting across different layers of a chain, Article 54 displaces the multiply-and-add calculation. A rule engine that only multiplies through the chain will report no beneficial owner in cases where Article 54 finds one. CRITICAL PATH · ART. 54	☐	☐	☐	☐
Produce the statement and justification where no beneficial owner can be determined Where beneficial owners cannot be determined after exhausting Articles 51 to 57, the entity must provide a statement to that effect, a justification of why and of what the uncertainty consists, and the details of all senior managing officials. A bare senior-managing-official entry with no statement does not meet this. ART. 63(4)	☐	☐	☐	☐

06 Enhanced due diligence and high-risk cases

7 CONTROLS

New named categories of enhanced due diligence, including a wealth-based trigger that did not exist before.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Build the wealth-management enhanced due diligence trigger Enhanced due diligence applies where a relationship involves handling assets of at least EUR 5,000,000 through personalised services, for a customer holding at least EUR 50,000,000 in total assets, excluding that customer's private residence, and the relationship is identified as higher risk. All three conditions are required. The duty binds credit institutions, financial institutions and trust or company service providers. Most private banking and wealth systems do not currently capture the total-assets figure at all. CRITICAL PATH · ART. 34(5) · CREDIT & FINANCIAL INSTITUTIONS · TCSPS, LEGAL & ACCOUNTING	☐	☐	☐	☐
Rebuild the PEP framework, including domestic PEPs and RCAs Senior management approval, source-of-wealth and source-of-funds establishment, and enhanced ongoing monitoring, with a defined de-listing rule for former PEPs rather than permanent flagging. ART. 42-46	☐	☐	☐	☐

06 Enhanced due diligence and high-risk cases CONTINUED

7 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Apply enhanced measures to high-risk third countries Country-specific countermeasures follow the Commission's listings. Your country risk model needs to update automatically when a listing changes, not at the next annual review. ART. 29–31	☐	☐	☐	☐
Define enhanced measures for correspondent relationships Cross-border correspondent relationships carry their own required measures, including approval and documented responsibilities. Article 36 covers credit and financial institutions, Article 37 covers crypto-asset service providers, and Article 39 prohibits correspondent relationships with shell institutions outright. ART. 36–37, 39 · CREDIT & FINANCIAL INSTITUTIONS · CRYPTO-ASSET SERVICE PROVIDERS	☐	☐	☐	☐
Set the simplified due diligence perimeter and evidence it Simplified due diligence is permitted only where the business-wide risk assessment supports lower risk. Record the justification per scenario. This is a frequently challenged area. ART. 33	☐	☐	☐	☐
Establish source-of-funds and source-of-wealth evidence standards Define what documentary evidence is acceptable, at what value, and who signs it off. Vague standards here are the most common cause of inconsistent EDD files. ART. 34	☐	☐	☐	☐
Route high-risk approvals to senior management with an audit trail Where senior management approval is required, the system must capture who approved, when, on what information, retrievable years later. ART. 34	☐	☐	☐	☐

07 Sanctions and targeted financial measures

5 CONTROLS

Screening quality is being pulled into the AML supervisory perimeter rather than treated as a separate discipline.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Screen customers and beneficial owners against targeted financial sanctions Screening must cover beneficial owners and controlling persons, not just the contracting party, and must run on an ongoing basis rather than at onboarding only. ART. 20(1)(D)	☐	☐	☐	☐
Tune matching quality and evidence the tuning Thresholds, transliteration handling, and fuzzy-match settings should be tested and documented. Supervisors increasingly ask for the test results, not the vendor's brochure. GOOD PRACTICE	☐	☐	☐	☐
Set list-update SLAs measured in hours, not days Define how quickly new designations propagate to live screening and to the back book, and monitor the actual latency. GOOD PRACTICE	☐	☐	☐	☐
Document the escalation and freeze workflow A true match requires immediate, defined action. Write the runbook, name the decision-makers, and rehearse it. GOOD PRACTICE	☐	☐	☐	☐
Run sanctions verification on its own clock, and on every new designation Verification that the Article 20(1)(d) conditions are still met runs at a frequency commensurate with risk, separately from periodic customer review. For credit institutions and financial institutions it must also be carried out upon any new designation. This does not replace the obligation to apply targeted financial sanctions. CRITICAL PATH ART. 26(4)	☐	☐	☐	☐

08 Monitoring, reporting and FIU cooperation

8 CONTROLS

Detection and reporting, with tighter response clocks than most teams are currently staffed for.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Confirm you can answer FIU information requests inside the deadline AMLR sets a short clock for responding to FIU requests: five working days in the standard case, with the possibility of shorter deadlines in urgent cases. Test whether you can actually retrieve and assemble a full customer file in that window. CRITICAL PATH · ART. 69	☐	☐	☐	☐
Calibrate transaction monitoring to the business-wide risk assessment Scenarios and thresholds should be traceable to identified risks and reviewed when those risks change. Keep the model documentation and the tuning evidence. ART. 26(1)	☐	☐	☐	☐
Define and staff the suspicious activity reporting workflow Detection, internal escalation, decision, filing and post-filing handling, with turnaround times and a quality-assurance step before submission. ART. 69	☐	☐	☐	☐
Enforce the tipping-off prohibition in process and in tooling Front-line staff must not be able to disclose that a report has been made. Check that case-management permissions and customer-facing systems actually prevent it. ART. 73	☐	☐	☐	☐
Handle abstention from transactions and post-report instructions Where you must refrain from carrying out a transaction pending FIU instruction, the operational and customer-communication path has to be pre-agreed. ART. 71	☐	☐	☐	☐
Track alert and case backlog as a board-level metric Backlog age is the fastest-moving indicator of an AML programme losing control. Report it, don't just measure it. GOOD PRACTICE	☐	☐	☐	☐

08 Monitoring, reporting and FIU cooperation CONTINUED

8 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Evidence the last-updated date for every customer against the hard caps The period between updates of customer information must not in any case exceed 1 year for higher-risk customers to which Section 4 measures apply, and 5 years for all other customers. Note the narrower scope: a high internal risk score does not by itself put a customer on the one-year clock. CRITICAL PATH · ART. 26(2)	☐	☐	☐	☐
Trigger review on the three named events, not only on the calendar Review and update customer information where there is a change in the customer's relevant circumstances, where you have a legal obligation during the calendar year to contact the customer about beneficial ownership or under Directive 2011/16/EU, or where you become aware of a relevant fact pertaining to the customer. ART. 26(3)	☐	☐	☐	☐

09 Records, retention and data protection

5 CONTROLS

Retention is unchanged in length but stricter in specificity, and it now has to coexist cleanly with GDPR.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Retain CDD records and transaction records for five years The five-year baseline retention period carries over. Confirm the clock start for each record type and that deletion actually happens at the end of it. ART. 77	☐	☐	☐	☐
Retain the reasoning, not just the documents Risk ratings, EDD justifications, approval decisions and discrepancy reports are all part of the file a supervisor will ask to see. Free-text notes scattered across systems will not survive that test. ART. 77	☐	☐	☐	☐
Reconcile retention with GDPR minimisation and erasure Internal policies must expressly cover personal data processing. Document the lawful basis, the retention justification, and how erasure requests are handled against the AML retention obligation. ART. 76	☐	☐	☐	☐

09 Records, retention and data protection CONTINUED

5 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Make records retrievable at speed and in usable form Retention is worthless if retrieval takes weeks. Given the FIU response clock, retrieval time is itself a control. Test it. ART. 69, 78	☐	☐	☐	☐
Set a policy for records held by outsourced providers and former vendors If you switch vendors before the retention period expires, you still owe the records. Write exit and data-return terms into every contract. ART. 9	☐	☐	☐	☐

10 Outsourcing, reliance and third parties

5 CONTROLS

Outsourcing survives, but with a notification procedure and a hard list of decisions you can never delegate.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Write a dedicated outsourcing policy with prior supervisory notification AMLR requires a prior notification procedure to the competent supervisory authority before an outsourcing arrangement begins. Build the lead time for that into vendor timelines now. CRITICAL PATH ART. 18	☐	☐	☐	☐
Ring-fence the functions you can never delegate Article 18(3) lists tasks that shall not be outsourced under any circumstances, starting with the proposal and approval of the business-wide risk assessment. Core risk and acceptance decisions, and the decision to report to the FIU, stay with you. Audit your current vendor arrangements against that list; some firms are already over the line. CRITICAL PATH ART. 18(3)	☐	☐	☐	☐
Run pre-contract due diligence on service providers and repeat it Assess capability, controls, sub-outsourcing chains and location of processing before signing, then re-assess on a defined cycle. ART. 18	☐	☐	☐	☐

10 Outsourcing, reliance and third parties CONTINUED

5 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Put written agreements and audit rights in place for every arrangement Written contracts, defined service levels, audit and inspection rights, and supervisory access. Verbal or implied arrangements will not pass. ART. 18	☐	☐	☐	☐
Set the conditions for relying on third-party CDD Reliance is distinct from outsourcing and has its own conditions: you remain responsible, and you must be able to obtain the underlying information immediately. ART. 48–50	☐	☐	☐	☐

11 Sectoral limits and specific obligations

10 CONTROLS

Rules that bite for particular obliged-entity types: cash, crypto, gambling, football.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Implement the EU-wide EUR 10,000 cash payment limit A Union-wide limit of EUR 10,000 applies to cash payments in commercial transactions, whether in a single operation or across several linked operations. Member States may set lower limits. Configure point-of-sale and finance systems, and build linked-operation detection. CRITICAL PATH ART. 80	☐	☐	☐	☐
Meet crypto-specific due diligence and transfer information requirements CDD obligations for crypto-asset transfers sit alongside the Transfer of Funds Regulation's travel-rule requirements. Confirm originator and beneficiary information is captured, transmitted and screened. ART. 19(3), TFR CRYPTO-ASSET SERVICE PROVIDERS	☐	☐	☐	☐
Address self-hosted wallet and anonymity-enhancing risk Set out how you treat transfers to and from self-hosted addresses and any anonymity-enhancing features, and evidence the risk rationale. ART. 40 CRYPTO-ASSET SERVICE PROVIDERS	☐	☐	☐	☐
Apply CDD at the gambling thresholds and link operations across sessions Collection of winnings, wagering of a stake, or both, above the applicable threshold triggers CDD. Cross-session and cross-channel linking is the hard part. ART. 19(5) GAMBLING	☐	☐	☐	☐

11 Sectoral limits and specific obligations CONTINUED

10 CONTROLS

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Confirm the thresholds that bring high-value goods traders into scope Traders in precious metals, precious stones and other high-value goods are obliged entities above defined thresholds. Confirm which of your product lines and transaction sizes cross them. ART. 3 · HIGH-VALUE GOODS TRADERS	☐	☐	☐	☐
Scope AML obligations for clubs and agents ahead of 2029 Transfers, agent commissions, sponsorship and ownership structures are the exposure points. Start with a risk assessment and an ownership map. ART. 3 · FROM 10 JUL 2029 · PROFESSIONAL FOOTBALL	☐	☐	☐	☐
Build threshold reporting for high-value goods sales Persons trading in high-value goods report to the FIU all sales of motor vehicles at EUR 250,000 or more, and watercraft or aircraft at EUR 7,500,000 or more, where the goods are acquired for non-commercial purposes. Reporting runs to the deadlines the FIU imposes, not to a date set in the Regulation. CRITICAL PATH · ART. 74(1), 74(3) · HIGH-VALUE GOODS TRADERS	☐	☐	☐	☐
Report high-value goods transactions you service for customers Credit institutions and financial institutions that provide services in relation to the purchase or transfer of ownership of those goods report the transactions they carry out for their customers. The duty is not limited to the trader. ART. 74(2) · CREDIT & FINANCIAL INSTITUTIONS	☐	☐	☐	☐
Know which of the two cash-limit carve-outs applies to you The EUR 10,000 limit does not apply to payments between natural persons not acting in a professional capacity, or to payments and deposits made at the premises of credit institutions, electronic money issuers and payment service providers. Payments in that second category above the limit must be reported to the FIU. ART. 80(4)	☐	☐	☐	☐
Subject legacy anonymous accounts to CDD before they can be used again Existing anonymous accounts, passbooks, safe-deposit boxes and anonymous crypto-asset accounts must be made subject to customer due diligence before they are used in any way. Dormant legacy products are the usual gap. ART. 79(1) · CREDIT & FINANCIAL INSTITUTIONS · CRYPTO-ASSET SERVICE PROVIDERS	☐	☐	☐	☐

12 Technology, data and operating model

6 CONTROLS

The practical build: what your systems, data and people have to be able to do by July 2027.

	IN PLACE	IN PROGRESS	NOT STARTED	N / A
Run a system and vendor gap analysis against AMLR Identify which obligations your current stack cannot meet, whether the inclusive UBO threshold, wealth-based EDD triggers, linked-operation detection, five-day file assembly, and get them into a vendor roadmap or a replacement decision this year. CRITICAL PATH · GOOD PRACTICE	☐	☐	☐	☐
Fix the data before the systems Most AMLR failures are data failures: missing ownership percentages, unstructured addresses, no total-assets field, customer records split across products. Profile the data first; the tooling decision follows from it. GOOD PRACTICE	☐	☐	☐	☐
Unify the customer view across products and entities Group-wide policies and five-day FIU responses both assume you can see one customer across the whole group. If that view does not exist, it is a build, not a config change. ART. 16, 69 · GROUPS ONLY	☐	☐	☐	☐
Track AMLA technical standards, and check whether direct supervision reaches you Every obliged entity should track AMLA's regulatory technical standards and guidelines as they are issued, because several AMLR obligations are only fully specified there. Direct AMLA supervision, beginning 2028, reaches only a selected cohort of credit and financial institutions. For everyone else the supervisor on 10 July 2027 is the same national authority as today. AMLA REG. 2024/1620 · AMLA SUPERVISION FROM 2028	☐	☐	☐	☐
Build the audit trail an examiner can follow unaided Every risk decision should be reconstructable from the system alone: what was known, what was decided, by whom, on what date, under which policy version. GOOD PRACTICE	☐	☐	☐	☐
Dry-run a supervisory examination before July 2027 Pick five customers across risk bands and assemble the complete file end to end under time pressure. It will surface gaps no policy review finds. GOOD PRACTICE	☐	☐	☐	☐

SCORING WHERE YOUR PROGRAMME STANDS

Score your readiness

Count your marks, then read the band that matches. In-progress counts a half. N/A items leave the denominator entirely.

IN PLACE	IN PROGRESS	NOT STARTED	N / A
× 1	× ½	× 0	Excluded

Readiness = (in place + half of in progress) ÷ (87 − N/A), as a percentage. Count your untouched **critical-path** controls separately: they set your sequence regardless of the headline number.

READINESS _____ %

Under 40%

Early stage. Foundations first: the business-wide risk assessment, the Article 11 appointments, and sizing the back book. Each one gates work downstream, and the back book is usually the largest single workload in the programme.

40 to 70%

In build. The programme is moving. Push the long lead times: supervisory notification for outsourcing, system and vendor changes, the inclusive ownership threshold, and back-book remediation.

Over 70%

Approaching readiness. Shift effort from controls to evidence. Can an examiner reconstruct each decision from the systems alone, without a person explaining it? Dry-run a supervisory examination on five real files.

Sequencing

Governance, the risk assessment and data remediation can start today. Ownership logic, remote onboarding and the back book are the long poles.

Where Shufti fits

AMLR asks you to prove onboarding, ownership, screening and monitoring as one connected file.

Shufti runs customer due diligence, business verification, AML screening and continuous monitoring on one owned stack, and the same integration accepts eIDAS electronic identification, European Digital Identity Wallet attributes and Qualified Electronic Signatures for the remote onboarding route.

Customer due diligence	Trigger logic, identity and attribute capture for natural persons and legal entities, deferred-verification limits, and the back-book remediation run.
Beneficial ownership	UBO discovery across Articles 51 to 57 on the inclusive 25% test, control tested alongside ownership, and the 14-day register-discrepancy duty in Article 24.
Sanctions and PEPs	Sanctions, PEP and adverse-media screening of customers and beneficial owners, with verification on its own clock and on every new designation.
Ongoing monitoring	The Article 26 clocks, event-driven refresh, evidenced last-updated dates, and an audit trail an examiner can follow unaided.

One glocal platform. The full compliance lifecycle, from sign-up to remediation. Every industry, every region, every use case.

Next step

Book a walkthrough to map this workbook against your current programme.
shuftipro.com/request-demo/

This workbook is a readiness aid, not legal advice. It summarises Regulation (EU) 2024/1624 (AMLR) and adjacent instruments in the EU AML package: Directive (EU) 2024/1640 (AMLD6) and Regulation (EU) 2024/1620 (AMLA). AMLD6 is transposed nationally, so controls touching registers, supervisory notification and sanctions may be stricter or add steps in your jurisdiction. Several AMLR obligations are still being specified through AMLA technical standards; re-check thresholds and procedural detail against the final texts before committing budget or design. Verify load-bearing citations against the EUR-Lex Official Journal text at eur-lex.europa.eu/eli/reg/2024/1624/oj/eng. Last reviewed 13 August 2026.

Shufti

Close the AMLR gaps before 10 July 2027

AMLR asks you to prove onboarding, ownership, screening and monitoring as one connected file. Shufti runs customer due diligence, KYB and UBO discovery, sanctions and PEP screening, and continuous monitoring on one owned stack, and the same integration accepts eIDAS electronic identification, EUDI Wallet attributes and Qualified Electronic Signatures. Walk through the platform configuration before a vendor decision.

Request a demo

Explore the platform

shuftipro.com
sales@shuftipro.com