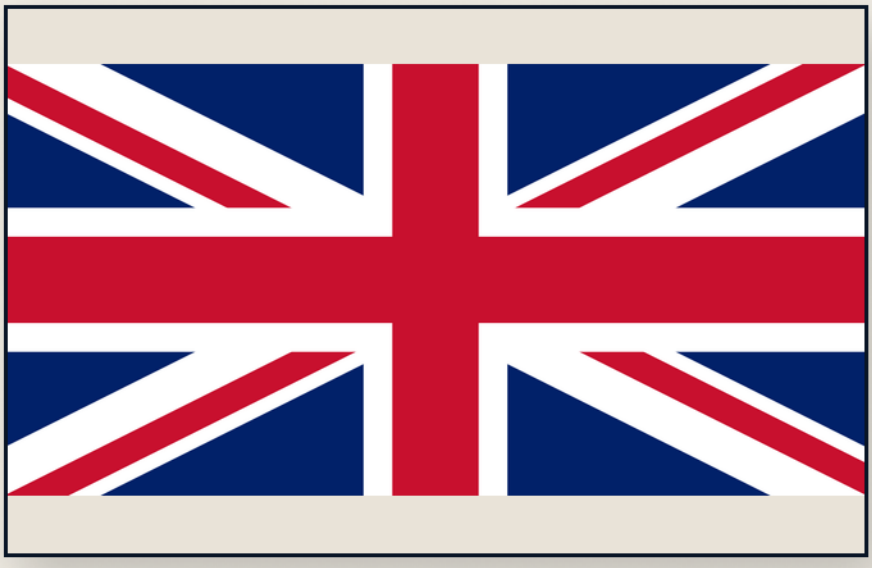
VOVE ID

VOVE COUNTRY CONTROL FILE

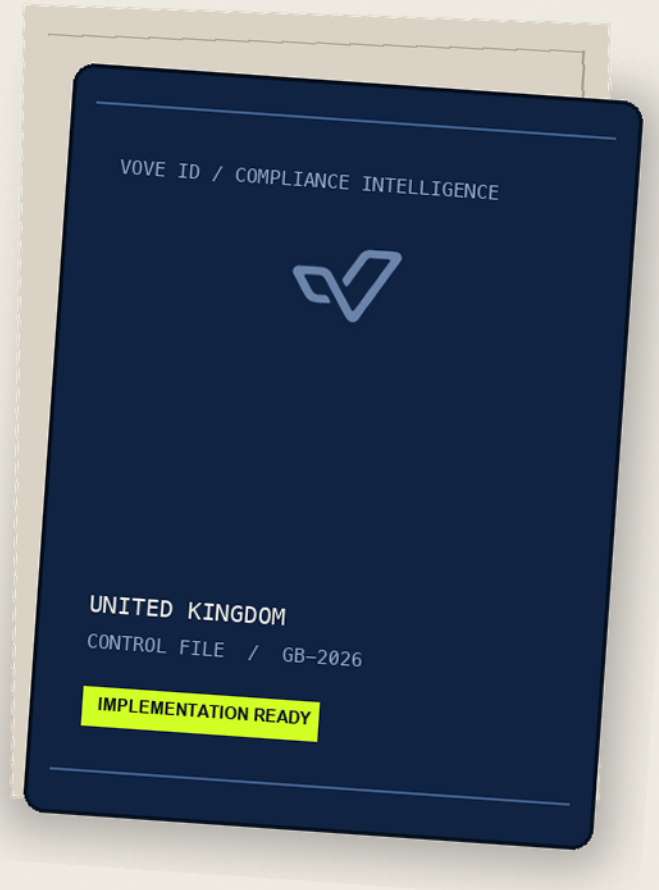
KYC / KYB / AML

2026 EDITION

UNITED KINGDOM



UNITED KINGDOM / GB



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

United Kingdom KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for financial institutions, payment and e-money firms, cryptoasset businesses, professional services and other teams entering the United Kingdom. It reflects the 30 June 2026 Money Laundering Regulations amendments and separates preventive controls, criminal reporting, sanctions, Companies House transparency, privacy and sector authorisation; applicability must be resolved before any control is treated as mandatory.

Primary AML rule	**Money Laundering Regulations 2017, as amended including SI 2026/621 effective 30 June 2026**
Financial intelligence unit	**UK Financial Intelligence Unit within the National Crime Agency (UKFIU/NCA)**
Suspicious activity report	**No monetary threshold; make a required disclosure as soon as practicable through the applicable internal or UKFIU route**
General occasional CDD	**GBP 12,000 or more from 30 June 2026; sector-specific triggers differ**
Funds-transfer CDD	**A transfer of funds exceeding GBP 800 triggers CDD; prescribed information rules also apply**
High-value dealers	**GBP 10,000 or more in cash is a scope and CDD trigger, not a universal threshold report**
AML beneficial ownership	**More than 25% shares or voting rights, ultimate management control or other control; tailored partnership and trust tests**
Companies House PSC	**More than 25% shares or votes, board-control rights, or significant influence or control under separate statutory conditions**
Core AML retention	**Five years from the record-specific transaction or relationship trigger, subject to limited longer retention and deletion rules**
Current sanctions list	**The UK Sanctions List has been the sole source for UK designations since 28 January 2026**
Cryptoasset businesses	**In-scope UK exchange and custodian-wallet providers must register with the FCA before starting**
FATF public lists	**The United Kingdom was not named on the FATF public lists reviewed 31 July 2026**

Scope and legal framework

The Money Laundering Regulations 2017 impose sector- and activity-specific AML, CFT and proliferation-financing preventive controls; The Proceeds of Crime Act 2002 and Terrorism Act 2000 create disclosure, money-laundering, terrorist-financing and tipping-off offences; Programme regulations made under the Sanctions and Anti-Money Laundering Act 2018 create financial-sanctions prohibitions, freezes, licences and reporting duties; The Companies Act 2006 and Economic Crime and Corporate Transparency Act 2023 reforms govern PSC transparency and phased Companies House identity verification; The UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025 govern KYC personal data, biometrics, breaches and transfers; The Payment Services Regulations 2017, Electronic Money Regulations 2011 and FCA rules govern payments, e-money, safeguarding and the current cryptoasset perimeter

FATF context

The United Kingdom has been a FATF member since 1990. As at 31 July 2026, it was not named on FATF's current public-list page for jurisdictions subject to increased monitoring or a call for action. FATF's United Kingdom page records the 2018 mutual evaluation and 2022 follow-up; absence from a public list is not a finding that every control is fully effective.

IMPORTANT

This checklist is general regulatory information, not legal advice, an authorization decision or a statement that every row applies to every UK business. It reflects primary and authoritative material reviewed on 31 July 2026. Confirm entity, activity, customer, transaction, legal form, UK nation, MLR supervisor, FCA permission, Companies House transition date, sanctions programme, privacy role, live reporting channel and later legal developments with qualified UK counsel and the competent authorities before launch.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

For every row, assign an owner, confirm whether the control applies, link the evidence, record gaps, and set a remediation date. A checked box is not evidence by itself.

01 / SCOPE	02 / DESIGN	03 / EVIDENCE	04 / REVIEW
Confirm institution, supervisor, product, customer and risk scope.	Map each obligation to a policy, system control or human review.	Retain the document, decision, timestamp, owner and rationale.	Test the control and update it when rules or risks change.

Checklist legend

CONTROL tells you what outcome to cover. IMPLEMENTATION ACTION translates that outcome into operational work. EVIDENCE suggests what an auditor or reviewer should be able to inspect. SOURCE points back to the primary rule or regulator guidance.

Minimum review record

Keep a compact decision record for each checklist row so a later reviewer can reconstruct what applied, who decided, and what evidence was inspected.

APPLICABILITY	OWNERSHIP	TRACEABILITY
Applicable, not applicable, or pending legal confirmation, with a short rationale.	Named control owner, reviewer, approval date and next review date.	Evidence link, source version, test result, gap status and remediation ticket.

Scope, authorities and licensing perimeter

Resolve every entity, activity, customer and UK nexus first. MLR supervision or registration does not replace FCA authorization, Companies House duties, sanctions compliance or another professional or devolved requirement.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
The MLRs apply to the relevant persons in regulation 8 acting in the course of UK business, subject to detailed sector definitions and exclusions.	Map each entity, product and service to regulations 8-15 and identify the FCA, HMRC, Gambling Commission or professional-body supervisor before launch.	Perimeter memorandum, legal-entity map, activity analysis, supervisor decision, exclusions and accountable owner.	MLRs, regs. 8-15 and 46
The 2026 MLR amendments generally took effect on 30 June 2026, while crypto correspondent rule 34A does not start until 1 February 2027.	Configure operative sterling thresholds and pooled-account controls now; place future crypto correspondent and 2027 control reforms on a dated change calendar.	Amendment assessment, effective-date register, configuration tests, future-change tickets and legal approval.	Money Laundering and Terrorist Financing (Amendment) Regulations 2026, reg. 1
Payment services and e-money issuance require the correct FCA authorization or registration unless another status or exclusion applies.	Classify each payment and e-money function, apply before regulated launch, and reconcile the permission with MLR supervisory status.	PSR and EMR analysis, application, FCA register extract, permissions matrix and launch gate.	PSRs 2017, regs. 4, 6 and Sch. 1; EMRs 2011, regs. 9 and 13; FCA payments guidance
An in-scope cryptoasset exchange provider or custodian wallet provider carrying on UK business must be registered with the FCA before starting.	Apply regulations 14A, 54 and 56 to the service and UK nexus; obtain registration before launch and separately assess financial promotions and the future FSMA regime.	Crypto perimeter memo, FCA application, registration decision, promotions review and 2027 transition plan.	MLRs, regs. 14A, 54 and 56; FCA, Cryptoassets AML/CTF regime
Where appropriate for size and nature, appoint a responsible board or senior manager, screen relevant employees and maintain independent audit; every relevant person also needs a nominated officer unless the sole-person exception applies.	Document appointments, notify the supervisor within 14 days where required, screen staff and operate risk-based independent assurance.	Appointment letters, supervisor notice, screening files, audit plan, reports and remediation evidence.	MLRs, regs. 21 and 24

Governance, risk assessment and control framework

A relevant person's programme must be demonstrably proportionate to its actual UK risks and current MLR obligations, including proliferation financing.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A relevant person must identify, assess and keep current written records of its money-laundering and terrorist-financing risks.	Assess customers, countries, products, transactions, delivery channels, size and nature; obtain approval and update for material change.	Business-wide risk assessment, source register, methodology, approvals, change log and control mapping.	MLRs, reg. 18
For a pooled account newly provided from 30 June 2026, understand purpose and use, test consistency with customer knowledge and risk, update CDD if needed, assess and mitigate ML/TF risk and consider account controls.	Document the measures and demonstrate to the supervisor that their extent is appropriate to the account's ML/TF risk.	Purpose and use assessment, consistency test, updated CDD, risk decision, controls, approval and supervisor evidence pack.	MLRs, reg. 29(10)-(13); SI 2026/621, reg. 15
A relevant person must separately assess proliferation-financing risk and maintain proportionate senior-approved policies, controls and procedures.	Map sanctions-evasion and proliferation exposure across ownership, trade, payments, geography and technology; connect risks to preventive controls.	PF risk assessment, senior approval, scenario inventory, sanctions mapping, tests and remediation log.	MLRs, regs. 18A and 19A
AML/CFT policies must cover risk management, internal controls, CDD, reliance, records, compliance monitoring, unusual activity and new technology.	Maintain a control inventory mapped to regulations 19-20, assign owners, test design and operation, and communicate changes across relevant branches.	Policy set, control matrix, board minutes, testing results, issues, training and branch attestations.	MLRs, regs. 19-20

Natural-person identification and verification

CDD triggers and evidence strength depend on the relationship, transaction and risk. The 30 June 2026 sterling thresholds must not be confused with universal onboarding rules.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
CDD applies when establishing a business relationship, on suspicion, when prior evidence is doubtful and at the prescribed occasional -transaction triggers.	Build a trigger matrix covering the general GBP 12,000 threshold, funds transfers above GBP 800 and sector-specific cash, casino, art, letting and crypto triggers.	Trigger matrix, workflow rules, linked-transaction logic, suspicion override, tests and exceptions.	MLRs, reg. 27 as amended by SI 2026/621, reg. 14
A relevant person must identify the customer, verify identity from reliable independent documents or information and assess the relationship's purpose and intended nature.	Define risk-based evidence standards, validate authenticity and independence, and record purpose, expected activity and decision before activation.	Identity evidence, source validation, customer profile, purpose record, timestamps and approval.	MLRs, reg. 28(2), (12)-(13) and (18)
Secure electronic identification can be a reliable independent source where it resists fraud and misuse and gives the assurance needed for the risk.	Assess digital identity assurance, fraud controls, accessibility, exception handling and evidence retention; do not treat vendor output as automatically sufficient.	Vendor assessment, certification or assurance evidence, test results, decision logs, exceptions and monitoring.	MLRs, reg. 28(19); HM Treasury, Using digital identities with the MLRs
A person purporting to act for a customer must be authorized, identified and independently verified.	Validate the mandate and signatory powers, identify and verify the representative, and connect every instruction to current authority.	Mandate, board authority, power of attorney, representative KYC, validation log and instruction record.	MLRs, reg. 28(10)
If required CDD cannot be completed, do not open the relationship or transact, terminate an existing relationship and consider a POCA or Terrorism Act disclosure, subject to regulation 31's express exceptions.	Block activation and transactions, escalate termination and repayment, document any privilege or insolvency exception and record the SAR and consent assessment.	CDD failure, restrictions, termination or repayment record, exception analysis, SAR decision and approvals.	MLRs, reg. 31

KYB, beneficial ownership and Companies House

Keep MLR beneficial-owner CDD, register-discrepancy reporting and the company's own PSC and identity-verification duties distinct. A Companies House record is not sufficient by itself for MLR beneficial-owner verification.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Corporate CDD requires verified registered details and reasonable measures on governing law, constitution, directors or senior managers, ownership and control.	Obtain current registry and constitutional material, verify status and address, map directors and senior operators, and understand every ownership layer.	Companies House extract, constitutional documents, status check, director list, ownership chart and verification log.	MLRs, reg. 28(3)-(5)
A body corporate's beneficial owners include individuals with ultimate management control, more than 25% of shares or voting rights, or other control; partnerships and trusts use separate tests.	Trace direct and indirect interests, voting arrangements and control to natural persons; apply regulations 5 and 6 by entity type.	Ownership calculations, control analysis, trust or partnership parties, source documents and reviewer approval.	MLRs, regs. 5-6
Only after exhausting all possible means may a relevant person treat the responsible senior manager as the body corporate's beneficial owner, with written records of actions and difficulties.	Escalate unresolved ownership, document every search and inconsistency, verify the senior manager and decide whether risk or failed-CDD rules prevent onboarding.	Exhaustion log, source searches, escalation, senior-manager verification, risk decision and approval.	MLRs, reg. 28(6)-(9) and 31
Before onboarding and at relevant later CDD or monitoring for a regulation 30A customer, collect the prescribed register excerpt and report any Schedule 3AZA material discrepancy through the specified registrar or HMRC route.	Compare register and CDD evidence, classify materiality, resolve false positives, submit through the correct route and retain the report.	Register excerpt, comparison, discrepancy analysis, submission, acknowledgement and resolution.	MLRs, reg. 30A and Sch. 3AZA

PEPs, EDD, source of wealth and remote onboarding

EDD applies to prescribed cases and other high-risk situations. Domestic PEP status is treated as lower risk absent other enhanced risk factors, but it still requires the regulation 35 process.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
EDD and enhanced monitoring are required in regulation 33 cases, including a FATF call-for-action-country relationship or transaction and any other situation presenting higher ML or TF risk.	Configure mandatory triggers and a documented high-risk methodology; do not automatically equate the FATF increased-monitoring list with the regulation 33 country trigger.	EDD rules, FATF list version, risk decision, enhanced checks, approvals and monitoring plan.	MLRs, reg. 33 as amended by SI 2026/621, reg. 19
When establishing or continuing a relationship with a PEP, family member or close associate, including an entity beneficially owned by the PEP, obtain senior approval, establish source of wealth and funds, and conduct enhanced monitoring.	Screen customers and beneficial owners, adjudicate matches, corroborate wealth and funds, approve the relationship and apply separate risk and EDD rules to other PEP transactions.	Screening result, relationship analysis, wealth narrative, funds evidence, senior approval, alerts and reviews.	MLRs, regs. 33 and 35(1)-(5), (13)
Domestic PEPs, their family members and known close associates are presumed lower risk than non-domestic PEPs unless other enhanced risk factors exist.	Apply the PEP controls proportionately, document additional risk factors and avoid either automatic rejection or unjustified simplified treatment.	Domestic-status proof, risk assessment, factor analysis, measures, approval and review schedule.	MLRs, reg. 35(3A) and (12)
Remote onboarding, anonymity-favouring products and new technology require risk assessment and, where higher risk exists, enhanced measures.	Test document and person match, fraud and impersonation risk, device and network signals, accessibility, manual escalation and vendor performance.	Remote-risk assessment, liveness or match tests, device data, exception files, vendor assurance and sampled outcomes.	MLRs, regs. 19(4), 28(19), 33 and 35; HM Treasury digital-identity guidance

Monitoring, suspicious activity and confidentiality

The MLRs create monitoring and internal-control duties; POCA and the Terrorism Act create role-specific disclosure offences. Case records must show when the statutory knowledge or suspicion test arose and why disclosure was timely.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Ongoing monitoring includes scrutiny of transactions, source of funds where necessary, and reviews that keep CDD documents and information current.	Calibrate monitoring to expected activity and risk, investigate linked behaviour, refresh CDD on change and record filing and non-filing decisions.	Scenario inventory, expected-activity profile, alerts, investigation notes, refresh history and dispositions.	MLRs, reg. 28(11)-(13)
A regulated-sector employee or nominated officer must make the applicable disclosure when role-specific conditions are met and information concerns a person engaged in, or attempting, money laundering or terrorist financing.	Escalate completed and attempted activity through the nominated officer and UKFIU/NCA routes, preserving privilege and reasonable-excuse analysis.	Attempted or completed activity, internal report, nominated-officer assessment, legal analysis, SAR reference and acknowledgement.	POCA, ss. 330-332 and 338; Terrorism Act 2000, ss. 19 and 21A; NCA SAR guidance
A required disclosure is made as soon as practicable; there is no general monetary threshold or universal fixed-day SAR deadline.	Timestamp receipt, investigation, threshold formation, internal escalation and UKFIU submission; use the current SAR Portal and document unavoidable delay.	Case chronology, evidence reviewed, suspicion rationale, portal submission, receipt and delay explanation.	POCA, ss. 330-332; NCA, Suspicious Activity Reports
Tipping-off and prejud icing-investigation offences apply when their statutory conditions are met, subject to defined disclosures and other exceptions.	Restrict case information, train staff, review customer communications and CDD continuation, and obtain legal approval for sensitive disclosures.	Access logs, communication review, training, legal decision, exception analysis and incident record.	POCA, ss. 333A-333D and 342; Terrorism Act 2000, ss. 21D-21G and 39; MLRs, reg. 28(14)-(15)

Payments, cash triggers and transfer information

The UK does not impose one universal transaction report. CDD thresholds, payment-transfer information and cryptoasset travel-rule duties must be configured separately.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
From 30 June 2026, general occasional transactions of GBP 12,000 or more and funds transfers exceeding GBP 800 trigger CDD, subject to sector-specific rules and linked operations.	Configure each threshold, currency conversion, linked-transaction detection, sector exception and suspicion override without treating it as a reporting threshold.	Rules specification, effective-date control, conversion source, test cases, alerts and CDD files.	MLRs, reg. 27(1)-(2); SI 2026/621, reg. 14
A high-value dealer's GBP 10,000 cash transaction is an MLR scope and CDD trigger, including linked operations; it is not a standalone universal cash report.	Identify qualifying goods activity and cash paid directly, indirectly or into an account for the seller's benefit; apply CDD before proceeding.	HVD perimeter analysis, cash aggregation, payer and beneficiary records, CDD and transaction decision.	MLRs, regs. 14 and 27(3)-(4)
Payment service providers must carry prescribed payer and payee information, detect missing data and respond to competent-authority enquiries under the retained funds-transfer framework.	Map originator, beneficiary and intermediary roles, mandatory fields, rejection or follow-up rules, sanctions screening and rapid retrieval.	Message-field mapping, validation tests, exception queue, follow-up records, screening and retrieval exercise.	MLRs, Part 7; retained Regulation (EU) 2015/847
Cryptoasset businesses must apply the UK travel rule, including prescribed originator and beneficiary information and the GBP 800 threshold for additional information in specified transfers.	Classify inter-business and unhosted-wallet transfers, collect and verify required data, manage missing information and report repeated failures to the FCA where required.	Travel-rule design, counterparty assessment, transfer messages, requests, decisions, FCA reports and records.	MLRs, regs. 64B-64G as amended by SI 2026/621, regs. 32-33

Targeted financial sanctions and asset freezes

UK sanctions are programme-specific. The UK Sanctions List supports detection, while the operative regulation determines designation effect, ownership and control, prohibitions, freezes, exceptions, licences and reports.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
UK persons worldwide and persons within UK territory must comply with applicable sanctions prohibitions under programme regulations made under SAMLA.	Map persons, ownership and control, products, counterparties, vessels, geography and conduct to every applicable programme before execution.	Sanctions perimeter, programme inventory, legal analysis, screening logs, ownership review and decision.	SAMLA 2018; OFSI, Financial sanctions general guidance
Since 28 January 2026 the UK Sanctions List is the only current source for all UK sanctions designations; the former OFSI Consolidated List is closed.	Screen against current UK Sanctions List data, monitor updates and remove any production dependency on the closed consolidated list.	List source, version and timestamp, update alerts, screening tests, migration record and quality checks.	FCDO, The UK Sanctions List; OFSI general guidance
Asset-freeze prohibitions can extend to entities owned or controlled by a designated person even if the entity is not separately named.	Investigate direct and indirect ownership and control, joint arrangements and practical control; freeze or reject as the operative rule requires.	Ownership chart, control evidence, legal conclusion, freeze or rejection, approvals and audit trail.	OFSI, Financial sanctions general guidance, ownership and control
A relevant firm must inform OFSI as soon as practicable when the applicable programme's knowledge or reasonable-cause reporting trigger is met and must report frozen assets as required.	Escalate potential breaches and designated-person assets immediately, preserve funds, use the current OFSI route and assess separate UKFIU disclosure duties.	Case chronology, asset record, freeze, OFSI report, licence or exception analysis, SAR assessment and acknowledgements.	Applicable sanctions programme regulations; OFSI, Financial sanctions general guidance, reporting obligations

9. RECORDS, RELIANCE AND REGULATOR ACCESS

Records, reliance and regulator access

Five years is the core MLR period, but its starting event and limited longer-retention rules differ. Outsourcing and reliance do not transfer legal accountability.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
CDD, discrepancy, transfer-information and transaction-reconstruction records must generally be kept five years from the relevant transaction completion or end of business relationship.	Map every record class to its exact trigger, retain reconstructable evidence and prevent early deletion across primary and backup systems.	Retention schedule, trigger dates, system configuration, legal holds, samples and deletion certificates.	MLRs, reg. 40(1)-(4)
A pooled-account customer must provide underlying-person and beneficial-owner identities on request and keep accurate, up-to-date written records of all monies paid in and out for five years from when each payment is known or reasonably believed complete.	Require the customer to provide law-enforcement information about itself and account management and use on request; preserve regulation 29 privilege and confidentiality treatment.	Information requests, ownership data, payment ledger, per-payment retention clocks, authority responses and privilege record.	MLRs, reg. 29(14)-(18); SI 2026/621, reg. 15
After the applicable period, MLR personal data must be deleted unless another enactment, court proceedings, data-subject consent or reasonable legal-proceeding need supports retention.	Run defensible deletion and exception review, record the legal basis for any extension and prevent indefinite AML-purpose retention.	Deletion workflow, exception register, consent or legal basis, approvals, logs and verification tests.	MLRs, reg. 40(5)
Reliance on a qualifying third party does not remove the relevant person's liability and requires immediate information plus arrangements for prompt document copies.	Confirm third-party eligibility, obtain the required CDD data immediately, test document retrieval and prohibit reliance in a FATF call-for-action country unless the group exception applies.	Reliance assessment, agreement, data receipt, retrieval test, country check, monitoring and exit plan.	MLRs, reg. 39
Using an agent or outsourcing provider does not transfer liability for CDD or register-discrepancy measures.	Contract for duties, access, security, audit, incident escalation and exit; test identity, screening, monitoring, reporting and retrieval end to end.	Responsibility matrix, contract, vendor diligence, control tests, incidents, remediation and exit package.	MLRs, reg. 39(7)-(8)

Privacy, biometrics, breaches and transfers

KYC necessity does not displace UK data-protection duties. Resolve controller and processor roles, lawful basis, special-category conditions, transparency, minimization and retention for each data use.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
UK GDPR principles and lawful-basis requirements apply to in-scope KYC data; from 19 June 2026 controllers must also facilitate complaints, acknowledge them within 30 days and respond without undue delay.	Map each data purpose, lawful basis, notice, recipient, access and retention; operate the DUAA complaint channel, investigation and outcome process.	Record of processing, lawful-basis register, privacy notice, data map, complaint log, acknowledgements and outcomes.	UK GDPR, arts. 5-6; DPA 2018; DUAA 2025, s. 103; ICO DUAA summary
Biometric data used to uniquely identify a person is special-category data and requires both an Article 6 lawful basis and an Article 9 condition.	Document necessity, proportionality and the special-category condition; minimize templates, separate uses, test accuracy and bias, and provide a non-biometric route where appropriate.	Lawful-basis analysis, Article 9 condition, biometric design, accuracy and bias tests, vendor terms and deletion proof.	UK GDPR, arts. 4(14), 6 and 9; DPA 2018; ICO biometric guidance
A DPIA is required before processing likely to result in high risk, including specified large-scale sensitive processing and biometric combinations.	Screen every identity and monitoring design early, complete and approve the DPIA where required, mitigate risks and consult the ICO if high residual risk remains.	Screening record, DPIA, necessity test, mitigations, DPO advice, approval and consultation record.	UK GDPR, art. 35; ICO, Data protection impact assessments
Notify a reportable personal-data breach to the ICO without undue delay and, where feasible, within 72 hours; notify affected people without undue delay when high risk exists and document every breach.	Start the clock on awareness, contain and assess risk, submit available facts within 72 hours, supplement promptly and preserve the full decision record.	Incident chronology, risk assessment, ICO report, affected-person notice, follow-up and breach register.	UK GDPR, arts. 33-34; ICO, Personal data breaches guide
A restricted international transfer requires an applicable UK adequacy regulation, safeguard or Article 49 exception in addition to ordinary UK GDPR compliance.	Map destinations and onward transfers, select and document the route, complete transfer-risk work where required, and contract for security, rights and exit.	Transfer map, adequacy or safeguard record, risk assessment, contract, supplementary measures and review.	UK GDPR, arts. 44-49; ICO, Guide to international transfers

Payments, agents and practical evidence packs

Turn the perimeter and legal controls into testable launch gates. Payment, e-money, cryptoasset, Companies House and MLR statuses overlap but are not substitutes for one another.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Covered payment and e-money firms must safeguard relevant funds under the PSRs or EMRs and the FCA supplementary regime effective 7 May 2026.	Apply CASS 10A and 15 and SUP 3A and 16 as relevant, identify and segregate funds, reconcile, maintain the resolution pack and submit required returns.	Safeguarding analysis, account documents, reconciliations, discrepancy log, resolution pack, audit and returns.	PSRs 2017, reg. 23; EMRs 2011, reg. 20; FCA PS25/12 and safeguarding guidance
A payment institution remains responsible for acts and omissions of agents and must register agents before they provide services; e-money distributors and agents have separate rules.	Perform due diligence, submit required FCA information, verify register status, contract for controls and supervise conduct, AML, complaints and safeguarding.	Agent assessment, FCA submission, register extract, contract, monitoring, complaints and termination plan.	PSRs 2017, regs. 34-36; EMRs 2011, regs. 33-36
An ACSP verifying identity for Companies House must be supervised for UK AML compliance, meet the verification standard and keep verification records for seven years.	Keep ACSP verification separate from MLR CDD, capture the evidence and prescribed statement, protect the personal code and calendar seven-year retention.	ACSP registration, supervision proof, verification record, Companies House submission, access controls and retention schedule.	Companies House, Tell Companies House you have verified someone's identity
Companies must identify and report PSCs, and mandatory identity verification applies to new directors and PSCs from 18 November 2025 with role-specific transition deadlines for existing persons.	Apply all five PSC conditions, file changes, capture each personal-code deadline, and distinguish Companies House verification from the business's own MLR CDD.	PSC analysis, filings, confirmation statement, personal-code evidence, deadline calendar and reconciliation to CDD.	Companies Act 2006, Part 21A and Sch. 1A; Companies House PSC and identity-verification guidance
Each checklist row requires a documented applicability decision, current source, control owner and reconstructable operating evidence before launch.	Mark every row applicable, not applicable or pending counsel confirmation; close blockers and obtain compliance, legal, privacy, security and product approval.	Completed checklist, rationale, source snapshot, owner sign-off, test result, gap ticket and launch approval.	MLRs, regs. 18-21, 24 and 28

SOURCES AND FURTHER READING

Verify against current official material

Primary law and regulator guidance control. Contextual VOVE ID reading is included to help teams operationalize the requirements and is not legal authority.

Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017
UK Legislation · Primary regulation
Open official source

Money Laundering and Terrorist Financing Amendment Regulations 2026
UK Legislation · Primary regulation
Open official source

June 2026 money laundering advisory notice
HM Treasury · Official government notice
Open official source

HMRC anti-money laundering guidance for supervised businesses
HM Revenue & Customs · Official supervisor guidance
Open official source

Using digital identities with the Money Laundering Regulations
HM Treasury and DSIT · Official government guidance
Open official source

Proceeds of Crime Act 2002
UK Legislation · Primary legislation
Open official source

Terrorism Act 2000
UK Legislation · Primary legislation
Open official source

Suspicious Activity Reports
National Crime Agency · Official FIU guidance
Open official source

Companies Act 2006
UK Legislation · Primary legislation
Open official source

Economic Crime and Corporate Transparency Act 2023
UK Legislation · Primary legislation
Open official source

People with significant control
Companies House · Official registry guidance
Open official source

2026 statutory guidance on significant influence or control
Companies House · Statutory guidance
Open official source

Identity verification for Companies House
Companies House · Official registry guidance
Open official source

Tell Companies House you have verified someone's identity
Companies House · Official registry guidance
Open official source

Changes to reporting material discrepancies to Companies House
Companies House · Official registry guidance
Open official source

Sanctions and Anti-Money Laundering Act 2018
UK Legislation · Primary legislation
Open official source

The UK Sanctions List
Foreign, Commonwealth & Development Office · Official sanctions list
Open official source

Current UK sanctions regimes
Foreign, Commonwealth & Development Office · Official government guidance
Open official source

Financial sanctions general guidance
Office of Financial Sanctions Implementation · Official regulator guidance
Open official source

Report a suspected breach of financial sanctions
Office of Financial Sanctions Implementation · Official reporting guidance
Open official source

Data Protection Act 2018
UK Legislation · Primary legislation
Open official source

UK General Data Protection Regulation
UK Legislation · Retained law
Open official source

Data Use and Access Act 2025
UK Legislation · Primary legislation
Open official source

DUAA summary of data-protection changes
Information Commissioner's Office · Official regulator guidance
Open official source

Biometric recognition guidance
Information Commissioner's Office · Official regulator guidance
Open official source

When a data protection impact assessment is required
Information Commissioner's Office · Official regulator guidance
Open official source

Personal data breaches guide
Information Commissioner's Office · Official regulator guidance
Open official source

New data-protection complaints law
Information Commissioner's Office · Official regulator guidance
Open official source

Guide to international transfers
Information Commissioner's Office · Official regulator guidance
Open official source

Payment Services Regulations 2017
UK Legislation · Primary regulation
Open official source

Information accompanying transfers of funds
UK Legislation · Retained law
Open official source

Electronic Money Regulations 2011
UK Legislation · Primary regulation
Open official source

Payment services and electronic money regulation
Financial Conduct Authority · Official regulator guidance
Open official source

Safeguarding requirements for payment and e-money institutions
Financial Conduct Authority · Official regulator guidance
Open official source

PS25/12 changes to the safeguarding regime
Financial Conduct Authority · Official regulator policy
Open official source

Cryptoassets AML and CTF regime
Financial Conduct Authority · Official regulator guidance
Open official source

Cryptoasset registration ahead of the new FSMA regime
Financial Conduct Authority · Official regulator guidance
Open official source

FATF United Kingdom country page
Financial Action Task Force · Official international assessment
Open official source

FATF black and grey lists
Financial Action Task Force · Official current-status source
Open official source

Document control

Version 1.4 / Published 31 July 2026 / Last reviewed 31 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general regulatory information, not legal advice, an authorization decision or a statement that every row applies to every UK business. It reflects primary and authoritative material reviewed on 31 July 2026. Confirm entity, activity, customer, transaction, legal form, UK nation, MLR supervisor, FCA permission, Companies House transition date, sanctions programme, privacy role, live reporting channel and later legal developments with qualified UK counsel and the competent authorities before launch.