Coadjute

AML Compliance Checklist

For UK Estate Agents

Built on the Coadjute Assured Compliance Framework (ACF) — an ISO 31000-aligned approach to AML risk management for UK property firms.

How to use this checklist

This checklist is structured around the three layers of the Coadjute Assured Compliance Framework. Working through it gives you complete coverage of HMRC's 34 risk indicators and 203 legal obligations — not just the ~5% covered by a digital ID app.

- **Layer 1** sets out the external requirements (laws, regulations and guidance you must comply with).
- **Layer 2** is how the firm organises itself to comply (governance, controls, training).
- **Layer 3** is the per-file workflow each client and transaction goes through. Items at every layer should be evidenced with dates, decisions and rationales.

Use the boxes as a working tracker, the framework as the structure, and the firm's records as the evidence.

LAYER 1

AML Law & Guidance

WHAT is required of you — the external regulatory baseline

1. Registration

- ☐ Registered with HMRC for AML supervision (Estate Agency Business)
- ☐ AML supervision fee paid and up to date
- ☐ Trading commenced only AFTER HMRC AML registration was approved

2. Awareness of Applicable Regulations

- ☐ Proceeds of Crime Act 2002 (POCA) — money laundering offences
- ☐ Terrorism Act 2000 — terrorist financing offences, failure to report, tipping off
- ☐ Money Laundering (ML), Terrorist Financing (TF) and Transfer of Funds Regulations 2017
- ☐ Sanctions and Anti-Money Laundering Act 2018
- ☐ HMRC sector guidance for Estate Agency and Letting Businesses (current edition + 2025 risk guidance)

3. Risk Assessment Context (external)

- ☐ National Risk Assessment (NRA) on Money Laundering and Terrorist Financing — read and cited in your BWRA
- ☐ National Risk Assessment of Proliferation Financing (PF) — read and cited (Reg 18A)
- ☐ FATF list of high-risk third countries (HRTC) — current version checked
- ☐ HM Treasury / OFSI sanctions lists — subscribed to the email alert service

LAYER 2

Business Governance & Controls

HOW your firm organises itself to comply — consistently and demonstrably

1. Leadership & Commitment

- ○ Board/owner accountability for AML is documented
- ○ Nominated Officer (NO) — also referred to as MLRO — appointed in writing
- ○ NO has sufficient seniority, authority and resources to perform the role
- ○ Named deputy or cover arrangement in place when the NO is unavailable
- ○ AML on the leadership agenda at least quarterly, with minuted decisions

2. Integration (AML Governance)

- ○ AML steps are embedded in your client onboarding process — not bolted on at the end
- ○ Higher-risk cases follow a documented escalation path with sign-off
- ○ AML responsibilities clearly assigned across roles (front-line, branch, NO, board)

3. Design — Business-Wide Risk Assessment (BWRA)

- ○ Written BWRA in place
- ○ Covers Money Laundering, Terrorist Financing AND Proliferation Financing (Reg 18A)
- ○ Assesses risk across all five framework dimensions:
  - ○ Service (sales, lettings, auctions, probate, multiple)
  - ○ Client (individual, company, trust, PEP, regulars vs one-off)
  - ○ Transaction (price band, source of funds, structure)
  - ○ Geography (where the client, property and funds are)
  - ○ Delivery channel (face-to-face, remote, via intermediary)
- ○ Tailored to your firm's actual services — not a generic template
- ○ Reviewed at least annually, with a dated record of every review
- ○ Updated whenever the business, services, customer base or geography materially change

4. Implementation — Policies, Controls & Procedures (PCPs)

- ○ Written PCPs covering all 24 PCP-related obligations in HMRC guidance
- ○ PCPs cover ML, TF and PF (Reg 18A)
- ○ Cash policy explicit and communicated (no-cash, or cash limits documented)
- ○ Reliance arrangements with third parties (digital ID vendors, auction platforms, conveyancers) are in writing
- ○ Each staff member has been issued the PCPs, with a dated acknowledgement log
- ○ PCPs reviewed and updated at least annually
- ○ Documented criteria for refusing a transaction (no ID, no SoF, suspicious circumstances)

5. Evaluation (Audit & Assurance)

- ○ Internal file reviews on a regular cadence (at least quarterly)
- ○ Mock audit on at least 10 random files annually — emulating an HMRC visit
- ○ Findings logged with corrective actions, owners and target dates
- ○ Comparison check: every Listing has a matching vendor AML check on file
- ○ Comparison check: every SSTC has a matching buyer AML check on file
- ○ Lessons fed back into the BWRA and PCPs

6. Improvement (Training)

- ○ All relevant staff receive AML training at least annually
- ○ Training covers ML, TF, PF, red flags, escalation & tipping off
- ○ Per-staff dated training record maintained — the audit trail
- ○ Refresher training when regulations, NRA or sector guidance materially change

7. Technology

- ○ Records system in use is fit for purpose and audit-ready
- ○ Digital backups of paper-based records
- ○ Access controls: only authorised staff can amend AML records
- ○ System captures dated decisions and rationales, not just documents

LAYER 3

AML Workflow (per file)

WHAT RISKS are managed on every client and transaction — the seven-step ISO 31000 workflow

1. Context — define the file scope

- ○ Service identified (sales, lettings, auction, probate, multiple)
- ○ Client type identified (individual, company, trust, PEP)
- ○ Transaction parameters captured (price, structure, source of funds)
- ○ Geography captured for client, property and funds
- ○ Delivery channel recorded (face-to-face, remote, via intermediary)

2. Identification — apply the 34 HMRC risk indicators

- ○ Customer risk indicators considered (profile, behaviour, PEP, structure, trust, REIT/OEIC, cash-intensive, JVs, PF-sanctioned regimes, terror-sanctioned)
- ○ Transaction risk indicators considered (super-prime, multiple, undervalue, complex/unusual structure, opaque entity, professional enabler, no commercial purpose, payment and SoF, bridging, common BOs, proof of ownership, co-owners, dual-use property, PF-sanctioned)
- ○ Geographical risk indicators considered (HRTC, overseas non-HRTC, intermediaries, virtual office)
- ○ Service risk indicators considered (multiple services on same asset, payments for EAB services, offshore ownership, auctions)
- ○ Delivery channel risk indicators considered (no face-to-face, third-party ID providers)
- ○ Anything unusual is flagged for structured analysis at Step 3

3a. Analysis — Standard Customer Due Diligence (CDD)

- ○ Verified identity of the seller / vendor
- ○ Verified identity of the buyer
- ○ Verified address (POA)
- ○ Beneficial owners identified (companies, trusts, multiple owners)
- ○ Land Registry confirms the vendor is the registered legal owner
- ○ Co-owners identified and checked
- ○ PEP screen completed
- ○ Sanctions screen completed (HMT/OFSI)
- ○ Source of funds (SoF) evidence collected and reviewed (note: Proof of Funds insufficient)
- ○ Source of funds (SoF) story evaluated for plausibility and gaps investigated and closed
- ○ Source of wealth (SoW) considered where appropriate
- ○ Video call completed for any client not met face-to-face
- ○ Date CDD was completed is recorded on the file (separate from ID document expiry dates)
- ○ CDD completed before the transaction proceeds

3b. Analysis — Enhanced Due Diligence (EDD), where required

- ○ Triggered for high-risk indicators, PEPs, HRTCs, complex structures
- ○ Additional documentation obtained
- ○ Additional questions asked and answers documented
- ○ Senior management approval recorded for the relationship
- ○ Increased scrutiny applied through the lifecycle

4. Evaluation — rate each indicator

- ○ Justification for each rating recorded on the file
- ○ Each in-scope indicator rated Red, Amber or Green using predefined criteria
- ○ Overall file risk rating recorded (high/medium/low)

5. Treatment

- ○ Decision recorded: Proceed / Proceed with conditions / Do not proceed
- ○ If conditional, the conditions are documented and tracked
- ○ Rationale aligns with the firm's risk appetite and approval thresholds

Layer 3 continues on next page...

6. Monitoring & Review

- ○ File monitored for material changes during the transaction
- ○ Indicators re-run when circumstances change
- ○ For lettings: ongoing monitoring repeated each new tenancy / renewal
- ○ Out-of-date documents not accepted
- ○ Risk rating updated where evidence changes the picture

7. Reporting & Record Keeping

- ○ Process in place to identify suspicious activity (red flags trained, escalation route)
- ○ Internal reports of suspicion are logged in writing (not handled verbally)
- ○ NO reviews internal reports and decides whether to escalate
- ○ SARs submitted to NCA where required
- ○ Copy of every submitted SAR is retained on file
- ○ DAML-SAR submitted where consent is required, before the transaction proceeds
- ○ Tipping off rules observed (no information given to the customer about the report)
- ○ Records retained for at least 5 years from the end of the business relationship
- ○ Records easily retrievable on request

HMRC AUDIT

If HMRC contacts you

What to have prepared when the visit letter arrives

1. Within ~2 weeks of the letter, send to HMRC:

- ○ Current written BWRA
- ○ All written PCPs (covering ML, TF and PF)
- ○ List of properties currently on the market
- ○ List of properties sold in the last 12 months (longer if requested)
- ○ Overview of the business and company structure
- ○ Description of the regulated work the business carries out

2. On the day of the visit, have the following ready:

- ○ ID for all employees from the business
- ○ List of all people who own or effectively direct the business
- ○ Banking and settlement records
- ○ Written staff training records and procedure documents
- ○ Suspicious activity reports — internal and submitted
- ○ Property files for any sample HMRC selects from your list
- ○ Access to the records system, with someone available to retrieve electronic records

3. Mindset

- ○ Files are complete and easy to evidence
- ○ Clear audit trail for every decision (who decided, when, on what basis)
- ○ Documentation matches the actual process followed
- ○ Voluntary disclosure of any known issues considered before the visit (reduces penalty)