# [COMPANY NAME]

---

# Customer Risk Assessment Policy

*CDD, EDD and Simplified Due Diligence Framework*

**CONFIDENTIAL**

Version 1.0 — 18 February 2026

Next Review: [Date]

Policy Owner: Money Laundering Reporting Officer (MLRO)

Classification: Confidential

# Contents

# 1. Introduction

## 1.1 Purpose

This Customer Risk Assessment Policy establishes the framework and methodology used by [Company Name] (the "Company") to assess, classify, and manage the money laundering (ML) and terrorist financing (TF) risks presented by its customers and business relationships. It defines when Standard Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and Simplified Due Diligence (SDD) measures are required to be applied.

This policy is a core component of the Company's wider AML/CTF framework and should be read in conjunction with the Company's AML/CTF Policy, Sanctions Policy, and Suspicious Activity Reporting Procedures.

## 1.2 Scope

This policy applies to all business relationships and occasional transactions involving the Company, across all products, services, delivery channels, and jurisdictions in which the Company operates. It is binding on all employees, contractors, and agents involved in customer onboarding, relationship management, transaction processing, or compliance functions.

## 1.3 Regulatory Basis

This policy is informed by the following legislative and regulatory requirements:

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) — Regulations 28–38 (CDD measures)
- Proceeds of Crime Act 2002 (POCA)
- Terrorism Act 2000
- Joint Money Laundering Steering Group (JMLSG) Guidance — Parts I and II
- FCA Financial Crime Guide (FCG)
- FATF Recommendations 10–12 and associated Interpretive Notes
- HM Treasury National Risk Assessment of Money Laundering and Terrorist Financing

# 2. Risk-Based Approach: Core Principles

The Company adopts a risk-based approach (RBA) to customer due diligence, as required by the MLRs 2017 and recommended by the FATF. The following principles underpin this policy:

**Proportionality:** The extent of CDD measures applied to any customer shall be proportionate to the assessed level of risk. Higher-risk customers receive more intensive scrutiny; lower-risk customers benefit from streamlined processes.

**Dynamic Assessment:** Risk ratings are not static. Customer risk shall be reassessed at defined intervals and in response to trigger events, ensuring that the risk profile remains current throughout the lifecycle of the relationship.

**Documented Rationale:** All risk assessment decisions, including the application of SDD, standard CDD, or EDD, and any risk rating overrides, shall be fully documented with clear rationale.

**No Relationship Without Assessment:** The Company shall not establish a business relationship or execute a material occasional transaction until a satisfactory risk assessment has been completed and the appropriate level of CDD has been applied.

**Escalation and Approval:** Higher-risk customers require approval from more senior personnel. The approval authority shall be commensurate with the risk rating assigned.

# 3. Customer Risk Factors

The Company's risk assessment methodology evaluates five principal risk factor categories. Each factor is assigned a weight reflecting its relative importance to the overall risk assessment:

## 3.1 Customer Type Risk

The nature and characteristics of the customer, including their legal form, regulatory status, reputation, and transparency of ownership structure. Certain customer types inherently present higher ML/TF risk due to the complexity of their structures, the opacity of their ownership, or their prevalence in financial crime typologies.

## 3.2 Geographic Risk

The jurisdictions associated with the customer, including their country of incorporation or nationality, countries of operation, and the origin or destination of funds. Geographic risk is assessed with reference to FATF evaluations, EU high-risk third country lists, HM Treasury designations, Transparency International Corruption Perceptions Index, and the Basel AML Index.

## 3.3 Product and Service Risk

The ML/TF risk inherent in the products and services to be utilised by the customer. Products that facilitate anonymity, rapid cross-border transfers, or high-value transactions without face-to-face interaction are considered higher risk.

## 3.4 Delivery Channel Risk

The method through which the business relationship is established and services are delivered. Non-face-to-face onboarding and third-party introductions carry additional risk due to reduced opportunity for direct verification.

## 3.5 Transaction Profile Risk

The expected nature, volume, value, and geographic pattern of transactions. Profiles involving high values, frequent international transfers, complex layering, or patterns inconsistent with the stated purpose of the relationship are considered higher risk.

# 4. Risk Scoring Methodology

## 4.1 Scoring Matrix

Each of the five risk factors is scored on a scale of 1 (Low) to 4 (Very High). The weighted sum of scores produces the customer's overall risk rating:

| Risk Factor | Weight | Low (1) | Medium (2) | High (3) | Very High (4) |
|---|---|---|---|---|---|
| **Customer Type** | 25% | Regulated entity, listed company | Established SME, sole trader with track record | Cash-intensive business, HNWI, trust | Shell company, bearer shares, unregulated entity in high-risk sector |
| **Geographic Risk** | 25% | UK / EEA low-risk jurisdiction | Non-EEA with equivalent AML regime | FATF grey-listed jurisdiction | FATF black-listed, sanctioned, or conflict zone |
| **Product / Service** | 20% | Standard retail products, basic accounts | Investment products, credit facilities | Private banking, correspondent banking, trade finance | Anonymous products, virtual assets, payable-through accounts |
| **Delivery Channel** | 15% | Face-to-face, branch-based | Online with verified ID | Non-face-to-face, third-party introduced | Fully remote, no physical verification possible |
| **Transaction Profile** | 15% | Regular, predictable, low value | Moderate value, some international activity | High value, complex structures, frequent international transfers | Unexplained wealth, structuring patterns, rapid movement of funds |

## 4.2 Calculating the Overall Risk Score

The overall risk score is calculated as follows:

**Risk Score = (Customer Type × 0.25) + (Geographic Risk × 0.25) + (Product/Service × 0.20) + (Delivery Channel × 0.15) + (Transaction Profile × 0.15)**

Example: A non-resident individual (score 3) dealing from a FATF grey-listed jurisdiction (score 3), using standard investment products (score 2), onboarded remotely (score 3), with moderate transaction volume (score 2):

*(3 × 0.25) + (3 × 0.25) + (2 × 0.20) + (3 × 0.15) + (2 × 0.15) = 0.75 + 0.75 + 0.40 + 0.45 + 0.30 = 2.65 → High Risk*

## 4.3 Risk Rating Thresholds and Due Diligence Requirements

The following table sets out the risk rating thresholds and the corresponding due diligence requirements, approval authorities, and monitoring intensity:

| Risk Rating | Score Range | Due Diligence Level | Approval Authority | Review Frequency | Ongoing Monitoring |
|---|---|---|---|---|---|
| **Low** | 1.00 – 1.75 | Simplified Due Diligence (SDD) | Onboarding team | Every 3 years | Standard automated monitoring |
| **Medium** | 1.76 – 2.50 | Standard CDD | Onboarding team | Annually | Standard automated monitoring |
| **High** | 2.51 – 3.25 | Enhanced Due Diligence (EDD) | MLRO / Compliance Manager | Every 6 months | Enhanced automated + manual review |
| **Very High** | 3.26 – 4.00 | Enhanced Due Diligence + Senior Management sign-off | MLRO + Board / Senior Management | Quarterly | Intensive manual review + automated alerts |

## 4.4 Risk Rating Overrides

In exceptional circumstances, the risk rating generated by the scoring methodology may be overridden. Overrides may only be applied upward (i.e. to increase the risk rating) or downward, subject to the following conditions:

- Upward overrides may be applied by any Compliance Analyst with documented justification
- Downward overrides require written approval from the MLRO, with a detailed rationale recorded on the customer file
- No downward override may be applied to a customer where EDD is mandatory under the MLRs (e.g. PEPs, high-risk third countries)
- All overrides are subject to periodic review and must be revalidated at each scheduled review

# 5. Standard Customer Due Diligence (CDD)

## 5.1 When CDD Is Required

Standard CDD measures must be applied in the following circumstances:

- Before establishing a business relationship
- Before carrying out an occasional transaction of €15,000 or more (or equivalent), whether in a single operation or several operations that appear to be linked
- Where there is a suspicion of ML/TF, regardless of any exemption or threshold
- Where there is doubt about the veracity or adequacy of previously obtained CDD data

## 5.2 CDD Requirements

The following table sets out the minimum CDD measures required for individual and corporate customers:

| CDD Measure | Individual Customers | Corporate / Legal Entity Customers |
|---|---|---|
| **Identity Verification** | Full name, date of birth, residential address verified against government-issued photo ID and proof of address | Registered name, company number, registered office, certificate of incorporation, articles of association |
| **Beneficial Ownership** | N/A (individual is the beneficial owner) | Identify all individuals holding ≥25% ownership or voting rights; verify identity of each beneficial owner |
| **Purpose & Nature** | Establish the purpose of the relationship and expected transaction activity | Establish nature of business, industry sector, purpose of relationship, and expected transaction profile |
| **Source of Funds** | Establish the origin of funds to be used in the relationship (e.g. salary, savings, investment returns) | Establish the origin of funds (e.g. trading revenue, investment, loan facilities) with supporting evidence |
| **Sanctions & PEP Screening** | Screen against UK, EU, UN, and OFAC sanctions lists and PEP databases | Screen entity, all directors, beneficial owners, and authorised signatories against sanctions and PEP lists |
| **Adverse Media** | Conduct adverse media screening for financial crime, fraud, and regulatory action | Conduct adverse media screening on entity, directors, and beneficial owners |

## 5.3 Timing of Verification

Identity verification must be completed before the business relationship is established or the transaction is carried out. In limited circumstances, verification may be completed during the establishment of the relationship if there is no risk of ML/TF, it is necessary to not interrupt normal business conduct, and verification is completed as soon as reasonably practicable after initial contact. The rationale for any delay in verification must be documented.

## 5.4 Failure to Complete CDD

Where the Company is unable to apply CDD measures to a satisfactory standard, it must not establish the business relationship, carry out the transaction, or continue the relationship. The Company shall consider whether a SAR should be filed with the NCA. All decisions to decline or exit a relationship on CDD grounds must be documented with clear rationale.

# 6. Enhanced Due Diligence (EDD)

## 6.1 When EDD Is Triggered

EDD is triggered in two ways: mandatory triggers prescribed by the MLRs 2017, and risk-based triggers identified through the Company's risk assessment process. The following table sets out all applicable triggers:

| Trigger Category | Specific Trigger | Mandatory / Risk-Based |
|---|---|---|
| **PEP Status** | Customer is, or is a family member or known close associate of, a Politically Exposed Person (domestic or foreign) | **Mandatory** |
| **High-Risk Jurisdiction** | Customer is established in, operates from, or has significant connections to a country identified on the FATF high-risk or increased monitoring lists, or designated by HM Treasury | **Mandatory** |
| **Correspondent Banking** | Establishment of a correspondent banking relationship with a credit institution or equivalent from a third country | **Mandatory** |
| **Complex / Unusual Transactions** | Transactions that are unusually large or complex, follow an unusual pattern, or have no apparent economic or lawful purpose (Regulation 33(1)(c) MLRs 2017) | **Mandatory** |
| **Risk Score** | Customer's weighted risk score exceeds the High threshold (>2.50) following the risk assessment methodology in section 4 | **Risk-Based** |
| **Adverse Media** | Negative media coverage linking the customer, beneficial owners, or connected parties to financial crime, corruption, sanctions evasion, or regulatory enforcement action | **Risk-Based** |
| **Complex Structures** | Customer uses complex ownership structures (layered entities, trusts, nominee arrangements) without clear commercial rationale, or where ultimate beneficial ownership is difficult to determine | **Risk-Based** |
| **Cash-Intensive Business** | Customer operates in a sector identified as cash-intensive by the National Risk Assessment (e.g. money service businesses, estate agents, art dealers, gambling operators) | **Risk-Based** |
| **Sanctions Proximity** | Customer has connections (business, personal, or geographic) to sanctioned individuals, entities, or jurisdictions, even if not directly sanctioned | **Risk-Based** |
| **Source of Wealth Concerns** | Customer's declared source of wealth is inconsistent with known profile, or wealth originates from higher-risk activities or jurisdictions | **Risk-Based** |
| **Transaction Anomalies** | Ongoing monitoring identifies transactions inconsistent with the customer's established | **Risk-Based** |

| | | |
|---|---|---|
| | profile, including structuring, rapid movement of funds, or unexplained third-party payments | |
| **Reluctance to Provide Info** | Customer is evasive, provides inconsistent information, or is reluctant to provide documentation requested as part of standard CDD | **Risk-Based** |

## 6.2 EDD Measures

Where EDD is triggered, the Company shall apply one or more of the following additional measures, proportionate to the assessed level of risk:

| EDD Measure | Description |
|---|---|
| **Source of Wealth Analysis** | Obtain and verify evidence of the customer's overall wealth, including employment history, business interests, inheritance, investment returns, or property ownership. Corroborate against independent sources. |
| **Source of Funds Verification** | Establish and evidence the specific origin of funds for each material transaction or deposit (e.g. bank statements, sale contracts, tax returns, dividend certificates). |
| **Enhanced Background Checks** | Conduct deeper background screening using multiple independent databases, open-source intelligence, adverse media searches, and where appropriate, third-party intelligence providers. |
| **Beneficial Ownership Deep Dive** | Trace the full ownership chain to identify all natural persons with ultimate control, including those below the standard 25% threshold where risk warrants. Verify identity of each with enhanced evidence. |
| **Senior Management Approval** | Obtain documented approval from the MLRO, Compliance Manager, or a designated member of senior management before establishing or continuing the business relationship. |
| **Enhanced Ongoing Monitoring** | Increase the frequency and intensity of transaction monitoring. Apply lower thresholds for alerts, conduct more frequent periodic reviews, and assign dedicated compliance oversight. |
| **Purpose of Relationship Review** | Conduct a detailed assessment of the stated purpose and intended nature of the business relationship. Challenge and corroborate the customer's explanation with documentary evidence. |
| **Country Risk Assessment** | Where geographic risk is elevated, assess the specific ML/TF risks of the relevant jurisdiction(s), including quality of AML regime, corruption levels, sanctions exposure, and FATF findings. |

The specific combination of EDD measures to be applied shall be determined on a case-by-case basis by the MLRO or Compliance Manager, taking into account the nature and severity of the risk indicators identified. The rationale for the selected EDD measures must be documented on the customer file.

## 6.3 PEP-Specific Requirements

In addition to the general EDD measures above, the following specific requirements apply to all PEP relationships (domestic and foreign):

- Obtain senior management approval before establishing or continuing the relationship
- Take adequate measures to establish the source of wealth and source of funds
- Conduct enhanced ongoing monitoring of the relationship throughout its duration
- Reassess PEP status at every periodic review; where a PEP ceases to hold a prominent public function, risk-based measures shall be applied for a minimum of 12 months

## 6.4 High-Risk Third Country Requirements

For customers connected to countries identified by the European Commission as high-risk third countries (or equivalent HM Treasury designations), the following minimum EDD measures apply:

- Obtain additional information on the customer and beneficial owners
- Obtain additional information on the intended nature of the business relationship
- Obtain information on the source of funds and source of wealth
- Obtain information on the reasons for the intended or performed transactions
- Obtain senior management approval for establishing or continuing the relationship
- Conduct enhanced monitoring of the business relationship by increasing frequency and timing of controls

# 7. Simplified Due Diligence (SDD)

## 7.1 When SDD May Be Applied

SDD may be applied only where the Company's risk assessment has determined that the risk of ML/TF is low, and the conditions set out in Regulation 37 of the MLRs 2017 are met. SDD is a concession, not an entitlement — the Company retains full discretion to apply standard CDD or EDD irrespective of the customer's assessed risk level.

SDD must never be applied where:

- There is any suspicion of ML/TF
- The customer is a PEP or connected to a high-risk third country
- The customer's risk score exceeds 1.75 (the Low threshold)

## 7.2 Eligible Customers and Conditions

| Eligible Customer | Conditions | Residual Obligations |
|---|---|---|
| UK-regulated financial institutions | Subject to MLRs or equivalent EU/EEA regulation; no adverse information | Ongoing monitoring for unusual activity; periodic re-screening |
| Listed companies on regulated markets | Subject to full disclosure requirements; transparent ownership | Confirm listing status annually; monitor for delisting or adverse events |
| UK government bodies / public authorities | Verifiable public entity with clear statutory purpose | Confirm status at onboarding; periodic verification |
| Low-risk pooled accounts | Held by regulated intermediary; underlying customers subject to CDD by intermediary | Confirm intermediary's regulatory status; obtain undertaking on underlying CDD |

## 7.3 SDD Measures

Where SDD is applied, the Company may:

- Reduce the frequency or depth of identity verification (but not eliminate it entirely)
- Reduce the extent of ongoing monitoring (but must still monitor for unusual or suspicious activity)
- Infer the purpose and nature of the relationship from the type of transaction or product

Even under SDD, the Company must be able to demonstrate that it has gathered sufficient information to establish that the relationship qualifies for simplified treatment. SDD does not constitute an exemption from CDD obligations.

# 8. Ongoing Review and Re-Assessment

## 8.1 Periodic Reviews

All customer risk assessments shall be reviewed on a periodic basis, with the frequency determined by the customer's risk rating (see section 4.3). Periodic reviews shall include a full refresh of CDD information, re-screening against sanctions, PEP, and adverse media databases, and a reassessment of the customer's risk score.

## 8.2 Event-Driven Reviews

In addition to scheduled reviews, customer risk assessments shall be reviewed immediately upon the occurrence of any trigger event:

| Trigger Event | Action Required | Timeframe |
|---|---|---|
| **Scheduled periodic review** | Full refresh of CDD, re-screening, risk re-assessment | Per review frequency in risk rating (quarterly to 3-yearly) |
| **Material change in customer profile** | Update CDD records, reassess risk rating, escalate if risk increases | Within 10 business days of becoming aware |
| **Transaction monitoring alert** | Investigate alert, update CDD if needed, consider SAR filing | Within 5 business days of alert generation |
| **Adverse media hit** | Assess relevance, update risk rating, initiate EDD if warranted | Within 5 business days of identification |
| **Sanctions list update** | Re-screen entire customer base; freeze and escalate any matches | Within 24 hours of list update |
| **Regulatory / law enforcement request** | Provide requested information; review and update customer records | Immediately upon receipt |
| **Change in jurisdiction risk profile** | Reassess all customers with connections to affected jurisdiction | Within 30 days of change |

## 8.3 Outcome of Reviews

Following any review, the risk rating may be confirmed, upgraded, or downgraded. Where the risk rating changes, the corresponding CDD level (SDD, CDD, or EDD) shall be adjusted accordingly. All review outcomes shall be documented, including the rationale for any change in risk rating.

# 9. Approval and Escalation Framework

The following matrix sets out the approval authority required for key decisions based on the customer's risk rating:

| Decision | Low / Medium Risk | High Risk | Very High Risk |
|---|---|---|---|
| **Onboarding approval** | Onboarding / Compliance Analyst | MLRO or Compliance Manager | MLRO + Senior Management / Board |

| | | | |
|---|---|---|---|
| **Risk rating override** | Compliance Manager | MLRO | MLRO + documented rationale to Board |
| **Relationship continuation (post-review)** | Onboarding / Compliance Analyst | MLRO or Compliance Manager | MLRO + Senior Management |
| **Exit / off-boarding decision** | Compliance Manager | MLRO | MLRO + Board notification |

Any decision that involves a departure from this policy (including risk rating overrides, exceptions to EDD requirements, or continuation of a relationship despite unresolved concerns) must be escalated to the MLRO with full documentation.

# 10. Record Keeping

The Company shall retain the following records for a minimum of five years from the end of the business relationship or the date of the occasional transaction, in accordance with Regulation 40 of the MLRs 2017:

- All CDD and EDD documentation, including identification evidence and verification records
- Risk assessment records, including scores, weightings, rationale, and any overrides
- Records of ongoing monitoring, periodic reviews, and event-driven reviews
- Approval and escalation records, including senior management sign-offs
- Correspondence and communications relating to the risk assessment process
- Records of decisions to decline, exit, or restrict customer relationships

# 11. Roles and Responsibilities

**MLRO:** Owns this policy. Responsible for final approval of high and very high risk customers, oversight of the risk assessment framework, reporting to the Board, and liaison with regulators and the NCA.

**Compliance Manager:** Day-to-day management of the risk assessment process. Reviews and approves medium and high risk assessments. Maintains the risk scoring methodology and calibrates thresholds.

**Compliance Analysts / Onboarding Team:** Conduct initial risk assessments, gather and verify CDD/EDD information, perform screening, and escalate cases as required by this policy.

**Relationship Managers:** Responsible for identifying changes in customer behaviour, profile, or risk indicators and reporting these to the Compliance team. Assist with gathering updated CDD information at periodic reviews.

**Senior Management / Board:** Approve the risk appetite and risk assessment framework. Receive and act upon MLRO reports. Provide sign-off for very high risk customer relationships.

# 12. Policy Review

This policy shall be reviewed at least annually by the MLRO and approved by the Board. Ad hoc reviews may be triggered by changes in legislation, regulatory guidance, the Company's business model, or the external risk environment. All amendments shall be recorded in the document control table below.

# 13. Document Control

| Version | Date | Author | Changes |
|---|---|---|---|
| 1.0 | 18 February 2026 | [MLRO Name] | Initial policy creation |

## Policy Approval

| Role | Name | Signature / Date |
|---|---|---|
| MLRO | [Name] | |
| Compliance Manager | [Name] | |
| CEO / Board Chair | [Name] | |