

High-Risk Entity Verification Guide (SOP)

KYC & Enhanced Due Diligence (EDD)

1. Purpose

This document outlines a standardized verification approach for reviewing high-risk entities during Know Your Customer (KYC) and Enhanced Due Diligence (EDD) reviews.

While supporting Excel workpapers demonstrate **what controls were applied** and **what decisions were reached**, this guide documents **how high-risk verification is performed** in a consistent, defensible, and audit-ready manner.

This SOP illustrates analyst-level investigative methodology using a representative high-risk import/export entity.

2. Scope

This guide applies to customers identified as **Medium-High or High Risk** during onboarding or periodic review, including cases involving:

- Complex or layered ownership structures
- Cross-border or offshore activity
- High-risk jurisdictions
- Adverse media exposure
- Expected transaction activity inconsistent with stated business purpose

3. Entity & Jurisdiction Verification

Registry Verification

The analyst verifies legal existence and registration status using relevant national and local business registries. Entity name, registration status, and business details are reviewed for consistency.

Any discrepancies or inactive indicators are documented and escalated.

Physical Address & Nexus Validation

OSINT-based address validation is performed using publicly available sources (e.g., satellite imagery and business listings) to assess:

- Commercial versus residential use
- Multi-tenant or virtual office indicators
- Plausibility of physical operations

Use of virtual or mixed-use locations triggers additional review and supporting documentation requests.

4. Ownership Transparency & UBO Identification

Ownership Layer Analysis

For entities with complex ownership structures, the analyst documents all ownership layers and attempts to trace control to **natural persons holding ≥25% direct or indirect ownership**.

Opacity & Red Flag Indicators

Indicators such as nominee directors, layered holding entities, or offshore structures increase opacity risk and require enhanced documentation.

Failure to identify controlling natural persons results in **High Risk classification** and escalation to EDD.

5. Adverse Media & Reputational Review

OSINT & Media Search

Structured adverse media searches are performed using Boolean logic (e.g., entity name combined with terms such as *investigation*, *fine*, or *customs violation*).

Assessment Criteria

Media findings are evaluated based on:

- Source credibility
- Relevance to financial crime or regulatory issues
- Recency and resolution status

Credible adverse media directly influences control outcomes and escalation decisions.

6. Source of Funds (SoF) vs Source of Wealth (SoW)

Source of Funds (Transaction Level)

Incoming funds are reviewed to confirm alignment with the stated business activity, supported by available contracts or transaction documentation.

Source of Wealth (Origin Level)

Owner wealth is evaluated separately. Where ownership transparency is limited or documentation is insufficient, the SoW assessment is marked as **Insufficient Evidence**, triggering enhanced review and escalation.

7. Reasonableness & Business Activity Alignment

A Reasonableness Test is applied to assess whether:

- Expected transaction volume aligns with the stated business model
- Geographic footprint aligns with operational claims
- Activity appears consistent with industry norms

Observed misalignment results in EDD triggers and escalation.

8. Final Decision Logic

In accordance with aggregation-based decision rules, escalation is mandatory when **two or more EDD triggers** are present.

In this case, escalation was required due to:

1. Exposure to high-risk jurisdictions
2. Complex ownership without confirmed natural person UBOs
3. Credible adverse media related to reputational risk

Escalation was policy-driven rather than discretionary.

9. Analyst Responsibility Statement

This SOP supports analyst-level verification and escalation recommendations.

Final onboarding, rejection, or continued relationship decisions are assumed to be approved by Compliance Management in accordance with internal governance frameworks.