Reviewability Diagnostic: specimen findings letter

This is a worked specimen of the diagnostic's output for ‘Mittenda Limited’, a fictional firm. Its documents and data are synthetic, derived from scenarios seen in practice; no engagement is reported, and the only content here that is not synthetic is the OpusDatum Risk register it quotes. It is stage one's output, the coverage review: what the documents evidence. How operations behave is stage two's ground, and nothing below claims to have watched them.

Documents reviewed

Mittenda's Financial Crime Framework (v1.2); AML/CTF Policy (v4.2); Risk Appetite Statement (v2.0); Customer Due Diligence Standard (v2.0); Transaction Monitoring Standard (v2.3); Sanctions Screening Standard (v5.3); Transfers of Funds and Crypto-Assets Standard (v3.2); Record Retention Policy (v1.4). The excerpts these findings cite are published in full, and every clause quoted below is indexed against them at mittenda.com/check.html. How far a review of documents reaches is set out at mittenda.com/working-papers.html. The set is the governing tier, the documents that answer to the board and the regulator; procedures are deliberately absent, since they implement what this tier requires, and whether they do is stage two's question; the business-wide risk assessment is a record of assessment, not a requirement, and enters at stage two as context. Every finding is adjudicated against this set and nothing else: Not evidenced means the governing tier is silent.

Specimen finding A: the name you verify and the name you transmit are never joined

Obligations

Regulation (EU) 2023/1113, Articles 4(1), 4(4) and 4(6) read together; for crypto-asset transfers, Articles 14(1), 14(6) and 14(8). 4(1) fixes the object, the information accompanying the transfer, of which the payer’s name is the first item; 4(4) requires its accuracy verified before dispatch against a reliable and independent source; 4(6) forbids execution before full compliance with the Article.

The risk

From the OpusDatum Risk register (this risk is published in full in the accompanying register extract): *“Risk that the originator's PSP or originator's CASP dispatches a transfer without having validly established the accuracy of the Article 4(1) / 14(1) … originator information before transfer, on the basis of documents, data or information obtained from a reliable and independent source. This may arise by omission, partial scope, non-reliable / non-independent source, stale evidence, late timing, wrong-record matching …”* This risk is why the duties are read together: its modes are the ways the name that travels stops being the name that was verified. Designated ‘strict’, one of the 23: no risk appetite can absorb it. The name accompanying the transfer carries a strict key risk of its own on the same Article, so this is a join defect between two of them.

Your documents

AML/CTF Policy §6.2: *“Customer identity is verified at onboarding against documents, data or information obtained from a reliable and independent source.”* The Transfers of Funds and Crypto-Assets Standard enumerates the accompanying fields, name, account and address, at §3.1 and §6.1; its §3.5: *“Where the identity of the originator has been verified … the accuracy … is deemed to have been verified, in accordance with Article 4(5) and Article 14(7).”*

State

NOT EVIDENCED · Article 4(1), 4(4) and 4(6) / 14(1), 14(6) and 14(8)

Basis

The Standard enumerates the Article 4(1) / 14(1) fields, and every row of that mapping closes. The Policy verifies the customer's identity; the duty verifies the accuracy of the accompanying information. §3.5 carries the join's whole weight on the Article 4(5) / 14(7) deeming, and the deeming presumes exactly what is missing: that the accompanying information is the record customer due diligence verified; no document requires the fields to be drawn from that record. The deeming is in the register, not outside it: three deeming risks, 31 modes, audited within this verification risk rather than given a slot of their own, and published in the extract. A keyword mapping marks every clause green and the duty's object is never verified. Every procedure downstream can comply with the Standard in full and still populate the message from the customer-editable display label, because nothing above the procedures says otherwise.

Operationally	The message can carry an account label, a trading name, or one holder of a joint account, and every downstream check will pass on a string your framework never verified. Screening runs faithfully against the wrong name; nothing ‘fails’; the record shows compliance.
What closes it	One requirement in the Standard: the Article 4(1) / 14(1) fields are drawn from the verified customer record, with the lawful fallbacks (trading name; joint holder) written down and evidenced. Every procedure beneath it inherits the rule. The diagnostic points; the engagement remediates.

Specimen finding B: record retention

Obligation	Regulation (EU) 2023/1113, Article 26(1): records of the accompanying information retained for five years from the transfer.
Your documents	Record Retention Policy §3.1: *“Records of transaction data, including payment messages and accompanying information, are retained for seven years from the date of the transaction.”*
State	**COVERED**
Basis	The duty is met as written and exceeded in period; the clause names the records the Article names. Nothing follows operationally. This is what Covered looks like: the duty, the clause, no daylight between them.

The verdict, and what a full letter contains

A full findings letter walks every obligation on the register, 120 in the Regulation and 94 arising through the EBA guidance, with the strict key risks leading, each finding in the format above, and closes with a verdict stated plainly: **your policy can carry a control-effectiveness review**, or **work regulation-first**, given per area. Coverage is never inferred from silence: a clause nobody can point to is Not evidenced, whatever everyone in the building believes. Stage two, the risk assessment of the key risks, starts from these findings: the same gaps, weighed against your business and the controls that actually run.

Andrew Travis
Director
OpusDatum Risk