Business-Wide Financial Crime Risk Assessment (v3.0, 2025 cycle)

Mittenda Limited · internal document · published as a specimen excerpt

Synthetic specimen. Mittenda Limited is a fictional firm. This document is invented, derived from scenarios seen in practice, and contains deliberate deficiencies for demonstration. It is not a template and must not be adopted.

Tier note. This is an assessment record, not a governing document: it records the assessment the Financial Crime Framework §5 requires. It sits outside the diagnostic's stage-one corpus, which reads the requirement-setting tier; it enters at stage two, as the context the assessed risks land in.

Document control: MTD-RSK-01 · owner: Head of Financial Crime (MLRO) · approved: the Board, 27 November 2025 · classification: Internal · assessment period: October 2024 to September 2025 · next assessment due: November 2026.

Version	Date	Change
3.0	November 2025	2025 annual cycle; crypto-asset services assessed in full
2.1	May 2025	Crypto-asset addendum on authorisation, pending the annual cycle
2.0	November 2024	2024 annual cycle

[Earlier versions omitted]

Contents

Sections in bold are excerpted below.

1. Methodology

1.1 This assessment covers each discipline of the Financial Crime Framework §2 across the risk categories of Directive (EU) 2015/849 Article 8: customers, products and services, delivery channels, geographies, and transactions. It has regard to the EBA's guidelines on money laundering and terrorist financing risk factors (EBA/GL/2021/02).

1.2 Inherent risk is rated before the operation of controls, on a four-grade scale: low, medium, medium-high, high. The direction records movement since the 2024 cycle. Ratings are the judgement of the assessment, evidenced in its working papers and reviewed by the Risk and Compliance Committee before Board approval.

1.3 The conclusions calibrate the Standards, including the calibration of the Transaction Monitoring Standard's scenarios to this assessment (§2.1 of that Standard), and the risk-based procedures beneath them.

2. Money laundering and terrorist financing

2.1 The assessment by category:

Category	Inherent rating	Direction	Basis
Customers	Medium	Stable	Consumers and small businesses on app-led onboarding; joint accounts; no correspondent banking or private banking relationships

Category	Inherent rating	Direction	Basis
Products and services	Medium-high	Raised	Payment accounts and credit transfers, including instant credit transfers; crypto-asset transfer services from April 2025, including transfers with self-hosted addresses
Delivery channels	Medium-high	Stable	Onboarding and servicing app-led and non-face-to-face throughout; electronic verification under the Customer Due Diligence Standard §4.2
Geographies	Medium	Stable	Customer base resident in Ireland and other Member States; cross-border reach through the correspondent network and, on the crypto-asset rail, counterparty providers in third countries
Transactions	Medium	Raised	Transfer speed rising with instant credit transfers; crypto-asset transfers with no de-minimis threshold

2.2 The rise in the products rating reflects the first full year of crypto-asset transfer services: transfers to and from self-hosted addresses, and the counterparty-provider population, are assessed as the rail's principal exposures, mitigated under the Transfers of Funds and Crypto-Assets Standard §6 and the Crypto-Asset Transfer Operations Procedure. The non-face-to-face channel remains medium-high; electronic verification at assurance level substantial or high is assessed as effective mitigation at onboarding.

2.3 Terrorist financing is assessed distinctly. Exposure is driven by transfer speed and reach rather than by customer profile; it is rated medium, stable, with mitigation resting on screening under the Sanctions Screening Standard and monitoring under the Transaction Monitoring Standard.

[Sections 3 onward omitted]