

The operational centre for financial-crime compliance, on Salesforce.

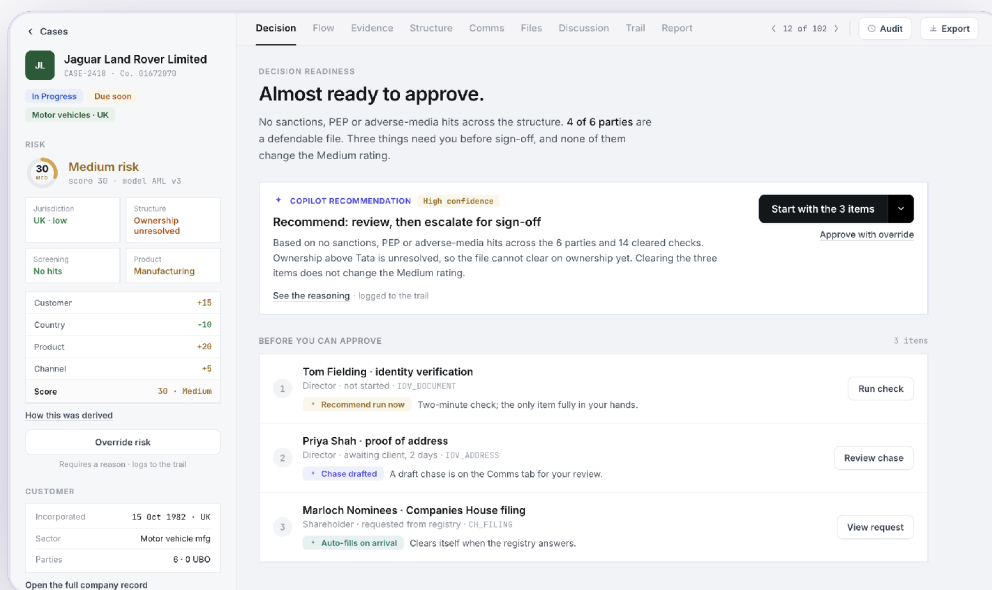
Investigate alerts, manage cases, score risk and produce audit evidence in one workspace. Ten specialised AI agents investigate every case before your analyst opens it. AI investigates, humans decide.

THE PROBLEM

Compliance teams spend most of their time on false positives, switching between six to eight disconnected tools and assembling audit evidence by hand. An investigation that should take minutes stretches to hours, and documentation takes longer than the investigation itself. When a regulator asks about a case from over a year ago, answering becomes a two-week project of CSV exports and screenshots. The MLRO carries personal liability for the one genuine hit lost in the noise.

WHAT COMPLIANCE HUB IS

A single workspace that replaces the patchwork. It runs on Salesforce as its data layer, orchestrates a network of screening and data providers, and puts a team of AI agents to work investigating each case before a human picks it up. Your analyst reviews structured, cited evidence and makes the decision. Nothing is decided autonomously.



The decision screen: Copilot recommends, your analyst decides, everything is logged to the trail.

PROOF IN NUMBERS

2 to 4 h → under 60 s

company research, as a 50+ field dossier

20-45 min → 2-3 min

to dispose of an alert

3-5 days → under 30 min

full business onboarding

1-3 h → under 45 s

individual due diligence

32 event types

immutable audit trail across 8 categories

209 countries

screening reach

WHAT YOU GET

Alert inbox. An AI-triaged queue ranked by risk, with SLA tracking and bulk resolution. Inbox-style, not a flat list.

Risk engine. FATF-aligned scoring across four dimensions, configurable rules, a 209-country risk database, champion/challenger testing.

Audit and reporting. An immutable trail of 32 event types across 8 categories, with one-click export for regulators.

Vendor orchestration. Connect screening, identity and company-data providers through one adapter framework. Run several in parallel, fail over automatically, and reuse a check across cases instead of paying for it twice. The audit trail is the same whichever provider ran the check.

Case management. A seven-status workflow with entity hierarchies, UBO trees, role-based assignment and three reviewer tiers.

AI investigation. Ten specialised agents across research, analysis and validation, plus an automated business-onboarding pipeline.

SLA monitoring. Real-time queue tracking, countdown timers, automatic escalation and role-based dashboards.

THE TEN AI AGENTS

Research

KYB Researcher, KYC Researcher, Alert Analyst, Document Classifier (30+ document types).

Analysis

Resolution Writer, Email Drafter, Risk Assessor (FATF scoring and EDD triggers).

Validation

Policy Parser, Model Optimizer, Vendor Mapper. Plus an automated onboarding pipeline end to end.

Each agent has a documented scope and creates an audit event for every action. Not a chatbot.

WHY IT IS DIFFERENT

- AI investigates first; your analyst reviews structured evidence, not a blank panel.
- It shows its work: every finding carries named, cited sources, and every AI action is flagged in the audit trail.
- One workspace for screening, monitoring, cases and audit, not separate platforms stitched together.
- No provider lock-in: swap a data vendor with a configuration change.
- It runs on your Salesforce security posture, so there is no new infrastructure to risk-assess.

BUILT FOR

MLROs and heads of financial crime, chief risk officers, compliance analysts and operations managers, from fintechs onboarding their first hundred clients to banks processing thousands of cases a month.

Where we are honest about the edges

Zenoo does not set your risk rating, does not self-learn your policy, and does not treat silence as clearance. It does not do transaction monitoring and does not file suspicious activity reports. Those decisions and duties stay with your compliance team.

Book a demo

30 minutes. Your data. No slides.

zenoo.com/get-a-demo