CONSORTIX

Whitepaper · 2026

How to Operate Your AML System Effectively

A practical guide for AML and compliance leaders who need more from the system they already have.

The Situation

The investment is already made.
The question is what you are getting from it

Most AML leaders we speak to are not planning a replacement. They are living with a system they bought three to seven years ago, one that was state of the art at the time of the RFP, passed through 18 months of implementation, and is now quietly accumulating problems that no one budgeted for.

The system works. Mostly. But the effort to keep it working is growing.

New regulations arrive and someone has to translate them into configuration changes. Source systems change and the data feeds need adjusting. Criminal typologies shift and the detection scenarios fall behind. Underneath all of it sit performance issues, unexplained alert spikes, and a support chain that, on close inspection, is not quite as solid as it looked on paper.

This document is about operating what you have effectively, closing the gap between the system you built and the system you actually need today.

Why the Gap Opens

AML systems drift for predictable reasons

Vendor support is narrower than it looks. Software vendors design support contracts around their product, not around your configuration. When they fix a bug, they fix something in the core software. When your scenario produces the wrong output because your data model changed in 2023, that is not their bug. It is your configuration problem, and their support team is not staffed or incentivised to solve it. Vendors are software businesses. Services compress margins and complicate valuations. Most would prefer you did not need them.

Internal IT does not understand AML. Your IT team has 40 priorities. AML is one of them, and not the one tied to revenue. They can restart a server and raise a ticket with the vendor. They cannot diagnose why your transaction monitoring is producing three times as many alerts as it should since the core banking upgrade in Q3. That requires AML domain knowledge combined with technical platform knowledge, a narrow combination that does not exist inside most banks.

The compliance and AML team absorbs both. They become the de facto IT support for their own system. They spend hours on workarounds, ticket management, and configuration archaeology instead of investigation and analysis.

This is technical debt. It compounds the same way financial debt does — paid in analyst time, in backlogs, in missed suspicious activity, in regulatory findings.

The Support Gap in Practice

When something goes wrong, the realistic options are usually these

Who	What they can do	What they cannot
Software vendor	Fix core software bugs	Debug your configuration, build your scenarios, tune your thresholds
Big Four consultant	Advise on strategy and regulatory interpretation	Provide hands-on platform support at SLA level
Local IT integrator	Handle infrastructure	Understand AML scenario setup and workflow dependencies
Internal IT	Raise tickets, escalate	Prioritise AML over core banking, loan origination, or anything revenue-generating
Your AML team	Know the business intent	Sustain the technical depth needed to own the platform

Banking groups that operate well typically use one of two models: either a dedicated internal team that owns the AML technology stack, or a specialised external partner providing SLA-based system support. Neither is universally right. The decision depends on scale, budget, and where the institution wants its internal expertise to sit.

For most teams, the middle ground works. The compliance team understands the system well enough to operate it day-to-day, while a specialised partner carries the technical depth for configuration changes, performance problems, and platform evolution.

Your Team's Role

What your AML team should own

The question most compliance teams ask during implementation is: *can we build our own scenarios?* The answer is yes. The better question is whether they should.

Building and maintaining detection scenarios requires understanding the data model, the detection engine, the test environment, and the performance trade-offs. There is a meaningful learning curve. For most teams, that time comes directly at the expense of what they are best placed to do: investigating alerts, analysing patterns, making decisions that regulation requires humans to make.

> **The practical threshold for most compliance teams:**

- Understand the data and scenario setup well enough to **validate outputs**
- **Tune existing scenarios**: adjust thresholds, modify lookback periods, change segment parameters
- Run **first-line diagnostics** when something looks wrong
- **Communicate precisely** with technical support and with the software vendor when escalation is needed

This keeps the team in control without pulling them away from investigation. It also makes the relationship with any external support partner more productive. The team can specify problems accurately and evaluate proposed fixes, rather than depending on the vendor's framing.

For larger, technically capable teams, there are additional tools worth considering, including AI-assisted scenario construction and completeness checking — but that is a separate conversation.

Your Support Partner

What a specialised support partner should deliver

SLA-based issue management

Defined response and resolution times for incidents, with a triage process that distinguishes configuration problems from software bugs from data issues. Not "we will look at it" — actual commitments.

Health checks — technical and business

Periodic reviews that cover both platform performance (query times, batch completion, data-feed integrity) and detection coverage (scenario calibration against current typologies, threshold tuning against population data, alert-to-SAR conversion rates).

Modification support

When regulation changes, when a new data source comes in, when the risk team identifies a coverage gap — someone needs to translate that requirement into configuration and test it properly before it goes live. This should be part of the support relationship, not a separate project that takes three months to scope.

Strong partners go further: they stay current on platform releases and regulatory developments and flag what is practically relevant to your setup. They understand the broader compliance technology stack — screening, CDD, case management, reporting — and identify where connections, redundancies, or simplifications would reduce operational burden. They prepare the ground for future improvements so that when the institution is ready to move, the foundation is already sound.

CONSORTIX

Where to Start

Start with a clear picture of where your system stands

Most institutions that engage Consortix for system support begin with an **AML system health check**. It covers three areas:

Platform health

Technical condition — query times, batch completion rates, data-feed integrity, and infrastructure stability.

Detection coverage

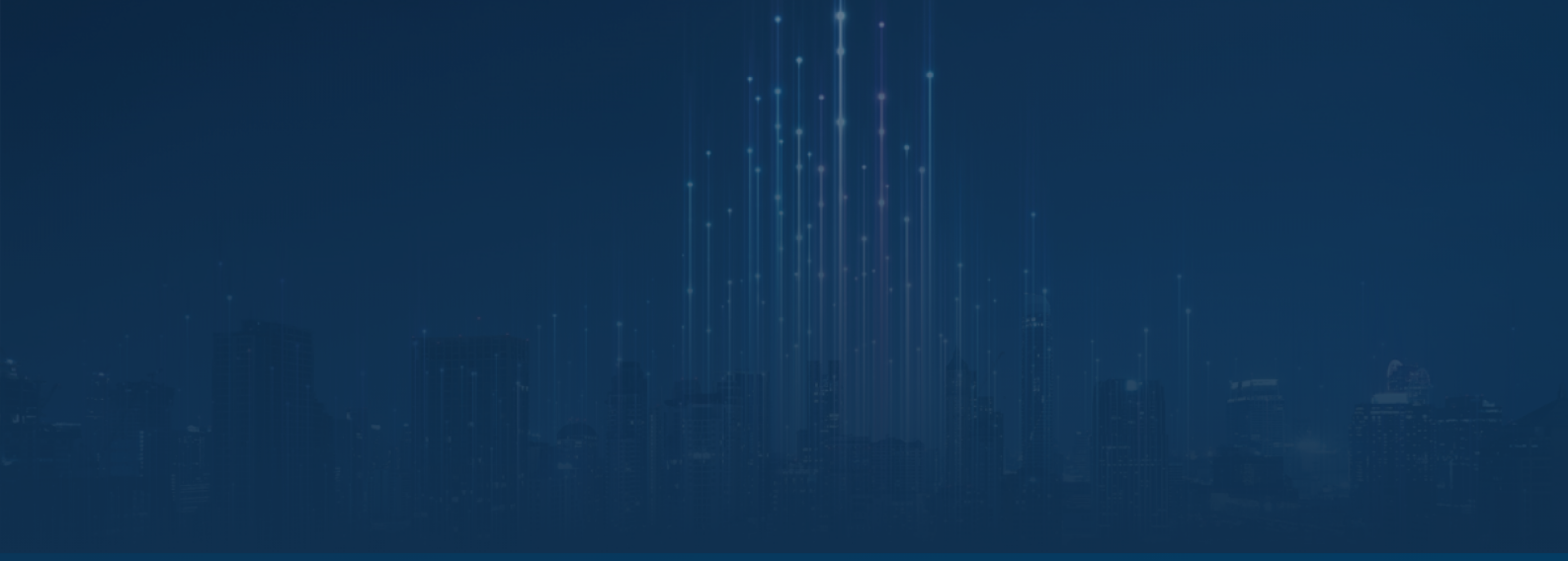
Current configuration measured against the regulatory and typological requirements the system is meant to address.

Support model

How the system is supported today — internal capabilities, vendor relationship, and the gaps between them.

It takes a few days. It produces a clear picture of where the system is working, where it is drifting, and what the practical options are.

Consortix has supported AML and financial crime compliance systems across Europe for over a decade. The platforms we work with include SAS, Lucinity, and Norkom/NetReveal. We do not advocate for a particular product — we work with what our clients have and recommend change only when the case is clear.



Get in Touch

Ready to find out where your AML system really stands?

Reach out to schedule a conversation about the health check,
or to discuss how Consortix can support your AML operations.

Tamás Sváb
CAMS
CHIEF EXECUTIVE OFFICER
tamas.svab@consortix.com
+36 30 412 8575

Csaba Simonyi
ACCOUNT EXECUTIVE
csaba.simonyi@consortix.com
+36 20 919 4959

ADDRESS
Consortix Zrt.
Czuczor u. 2–10
1093 Budapest, Hungary

WEB
consortix.com
info@consortix.com

CONSORTIX