REGTECH-DRIVEN.
HUMAN-GUIDED.

JurisComply
A member of JurisTax Group

AML SURVIVAL GUIDE 2025-2026

10 CRITICAL INSPECTION FAILURES - AND HOW TO FIX THEM FAST

AMLX Edition

Executive Summary

Regulators do not reward effort; they reward evidence. The companies that pass inspections in 2025–2026 share three traits:

- ✓ **Standardised, risk-based AML frameworks mapped to law and guidance.**
- ✓ **Automated evidence trails (who did what, when, based on which data).**
- ✓ **Continuous monitoring with clear KPIs, not annual 'catch-up' sprints.**

This guide distils 10 frequent inspection failures we observe across banks, DFIs and CSPs, and gives fast, practical remedies you can apply within weeks.

Part I: The 10 Most Common Inspection Failures (and Remedies)

1. Business Risk Assessment That Does not Reflect Reality

Most companies treat the Business Risk Assessment (BRA) as a compliance document, not a business tool. It often sits on a shelf, copied from someone else, or written years ago and never updated. When the regulator asks how your risks have evolved since your last assessment, that is when the gap shows.

A strong BRA should tell a story:
What types of clients do you serve? Which ones carry higher AML exposure? How do your products, markets, and delivery channels contribute to that risk? And, crucially, how often do you re-evaluate it?

If your BRA does not answer those questions in plain language, refresh it. Make sure the board discusses and approves it, and that everyone internally knows the top three risks to monitor. When the next inspection comes, you will be judged less on form, and more on whether your assessment matches the business you actually run.

2. Weak Client Due Diligence (CDD) Practices

Many businesses underestimate how much of compliance starts and sometimes ends with good client onboarding. Missing UBO charts, outdated documents, or vague "source of funds" explanations are still among the top reasons companies fail inspections.

A regulator does not expect you to know every client's life story, but they do expect you to show that you asked the right questions and verified the right information based on the client's risk level. Low-risk clients can be straightforward; high-risk clients need deeper checks and evidence.

Review your onboarding templates, refresh your checklists, and ensure every file tells a consistent story: who the client is, where their money comes from, and how you verified it. It is not paperwork, it is protection.

3. Transaction Monitoring That Does not Match the Business

Many companies have transaction monitoring systems that look impressive but do not actually reflect how their business operates. Generic rules and random thresholds create noise — hundreds of false alerts — while genuine suspicious activity gets missed.

Effective monitoring is about relevance, not volume. The scenarios, thresholds, and alerts should reflect your real exposure — the size of your transactions, the markets you operate in, and the types of clients you serve.

Regulators increasingly ask, "How does your monitoring relate to your Business Risk Assessment?" If your team cannot answer that question clearly, it is time to recalibrate.

4. Poor Sanctions and PEP Screening

Screening failures are among the easiest for regulators to spot. Infrequent re-screening, weak matching logic, and inconsistent handling of alerts are red flags. The risk? You miss a sanctioned individual or politically exposed person (PEP) and do not even realise it.

Modern screening is not just about name-matching. It is about frequency, accuracy, and documentation. You must be able to show when screening took place, how matches were cleared, and who approved the decisions.

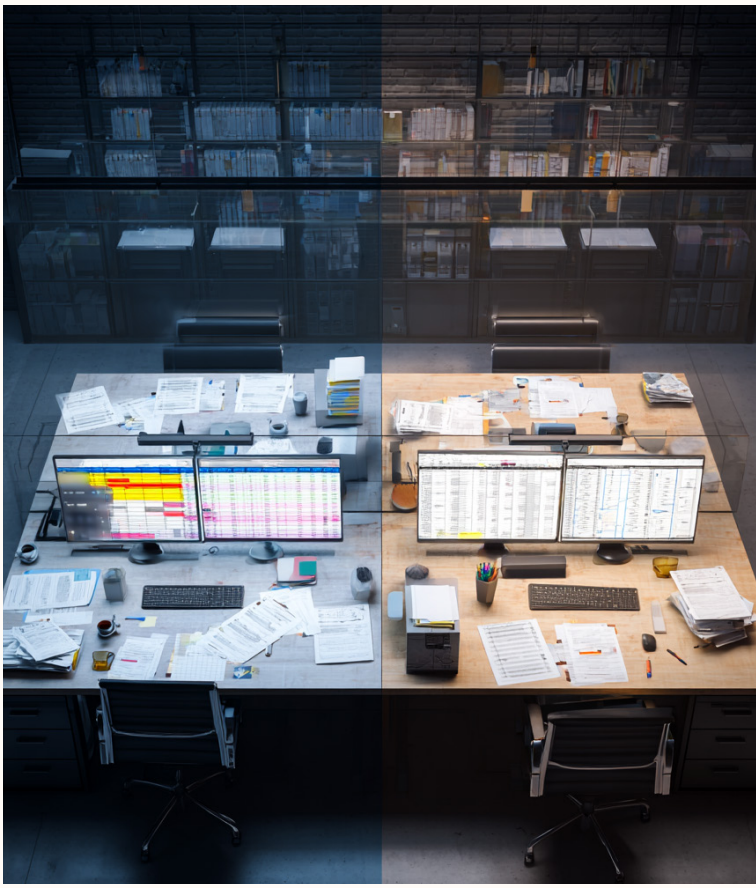
Invest in a good screening system, define how often each client segment is re-screened, and log every alert's outcome. Regulators are not impressed by brand names; they are impressed by traceability.

5. Internal Audit That Checks Boxes, Not Risks

Some companies still run their AML audit as a yearly routine, same scope, same checklist, same findings. Regulators see through that immediately.

A real audit should reflect your current risks. If your BRA changed, your audit scope should change too. The goal is to test where failure is most likely, not where it is easiest.

An independent audit function, whether internal or outsourced, must be risk-based, evidence-driven, and tracked. Findings without follow-up are worse than no audit at all. Make sure every recommendation has an owner, a due date, and a closure proof.



6. Governance Without Insight

Boards often receive “AML reports” full of statistics and pages of tables, but no insight. When the regulator asks directors to explain key trends or risk changes, the answers are vague or inconsistent.

A strong governance structure provides clarity. Senior management should regularly review key indicators such as alert volumes, STR conversions, and overdue KYC files, not to admire numbers, but to act on them.

When reporting to your board, simplify. What changed? Why? What decisions need to be made? That’s the level of governance regulators now expect.

7. Policy and Procedure Overload

In many companies, there are too many policies, too many templates, and no one knows which version to use. That chaos creates real compliance risk.

Regulators now look at how you manage your own documentation. Do you have one central policy library? Can you prove which version was in use at a given time? Can every staff member access the latest form?

Simplify and standardise. Keep a single policy register, assign version owners, and ensure all staff of the company have read the current versions. This small fix eliminates one of the most embarrassing inspection failures.

8. Training That Does Not Change Behaviour

Training should create awareness, not tick a box. Many companies show 100% completion rates but still face repeated compliance breaches.

Regulators no longer care how many employees completed training; they care how much staff actually understood. Training must be role-based, with practical examples and a short test to measure comprehension. Anyone who does not pass should retake it, not as punishment, but as reinforcement.

Show that you are serious about competence, not just attendance. That’s what inspection teams respect.

9. Weak STR Processes and Inconsistent Decision-Making

Filing a Suspicious Transaction Report (STR) is not just a regulatory step, it is a test of your organisation's judgment. The most common failures are delays, poor narrative quality, or internal confusion about when to report.

A solid STR process has three things: clear escalation paths, quality narratives that explain the "who, what, when, why, and how," and timely submission. Regulators read these reports carefully. They can tell when a company has thought through its suspicion and when it is just following a script.

Train your team on how to build a strong STR narrative. It is the one part of compliance where words really matter.

10. Poor Record-Keeping and Audit Trail

When regulators ask for proof, they do not just want to see that something was done, they want to see how it was done, when, and by whom. Too many companies cannot show that trail.

Record-keeping is not administrative, it is defensive. Keep your documents structured, with clear ownership and retention rules. Every key decision from onboarding, to alerts, to audits, should leave a digital footprint showing the rationale and the reviewer.

If your systems do not do that automatically, fix them now. A missing trail can make even a compliant action look suspicious.

Final Thoughts

Every one of these failures has the same root cause: fragmented systems and unclear ownership. Regulators are no longer impressed by effort; they look for structure, traceability, and accountability.

By building consistent frameworks, empowering your compliance team, and using tools like AMLX to automate documentation and evidence generation, your business will move from "reactive compliance" to proactive inspection readiness.

Part II: The JurisComply 90-Day Readiness Model

Compliance does not have to be chaotic or endless. Our proprietary 90-day model, powered by AMLX, helps companies move from reactive compliance to inspection-ready confidence.

Stabilise

This layer focuses on aligning your people, templates, and decision-making so that everyone works from the same source of truth. AMLX provides the structure to unify processes and reduce confusion around documentation, risk assessment, and approvals.

Systemise

Once stability is achieved, processes must become predictable. This phase embeds consistency, oversight,and accountability across the company. We introduce a system that connects policies, monitoring rules, and reporting ensuring decisions are evidence-based and traceable.

Demonstrate

Inspection readiness is not about having more data; it is about being able to show it clearly. In this phase, management gains board-level visibility through dashboards and AMLX audit-ready reporting. Every compliance action becomes verifiable, measurable, and regulator confident.

The JurisComply 90-Day Readiness Model is implemented exclusively for our clients through guided AMLX onboarding and advisory engagements. It is what turns documentation into proof, policy into performance, and compliance into a competitive advantage.

JURISCOMPLY

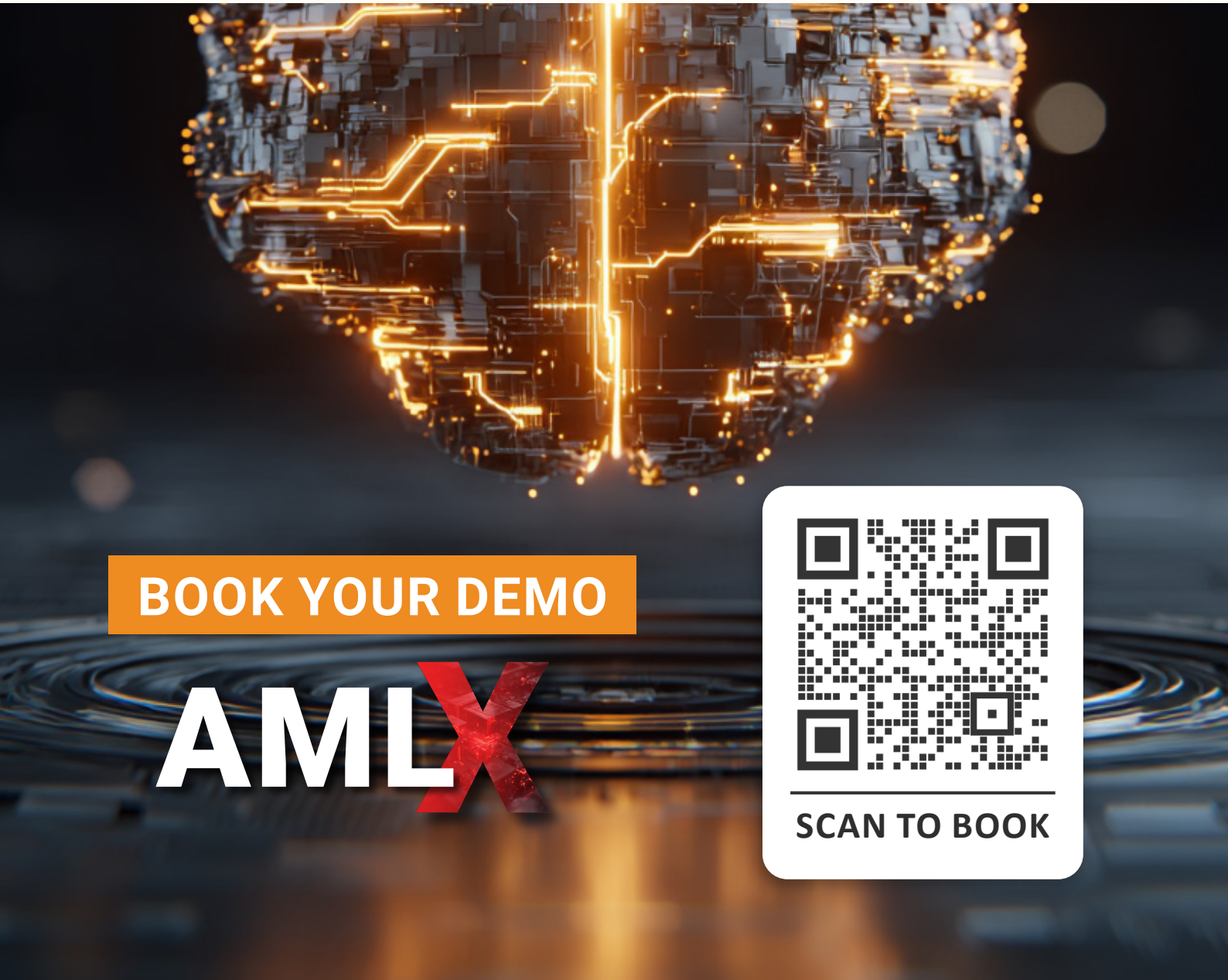
BUILT BY COMPLIANCE OFFICERS. POWERED BY AI.

(+230) 5944 8503 | (+230) 5919 0465

juriscomply@juristax.com

www.juriscomply.mu

JurisComply



BOOK YOUR DEMO

AMLX

SCAN TO BOOK