Sygno

Transaction Monitoring under AMLA's Draft Guidelines

Overview: Requirements and capabilities

Whitepaper | August 2026

About this paper

Article 26 AMLR requires obliged entities to conduct ongoing monitoring of every business relationship, and Article 26(5) mandated AMLA to issue guidelines on how that should be done. This paper deals with **Guideline 2:** what is asked of a **transaction and activity monitoring framework.** It reflects the consultation paper of 3 June 2026, on which consultation closes on 3 September 2026, with final guidelines expected in Q4 2026.

Overview: This is the **overview of a set of three papers**. It is an extended management summary of what the guidelines ask and what follows from that for an institution preparing for AMLR. Two detailed papers carry the full analysis, provision by provision:

Part 1: What the framework must detect, and what it measures against

Part 2: What the framework must demonstrate, and how it stays effective

The requirements group into eight themes across the two detailed papers. They converge on **six core capabilities** that an institution has to have in place under AMLR.

Part 1

What the framework must **detect** and what it **measures against**

1. A single view of the customer
2. What deviation is measured against
3. Detecting across time and networks
4. Design and its limits

Part 2

What the framework must **demonstrate** and how it **stays effective**

5. What effectiveness means
6. Staying fit for purpose
7. Explainability, and to whom
8. Data, tools and responsibility

converge on

Six core capabilities

1. All customer behaviour in one assessment
2. Detection reference points derived from the data
3. Detection logic generated from the institution's own data
4. A complete record of what the framework did and why
5. Performance measured on evidence
6. The framework learns from what it finds

The six core capabilities

Article 26 AMLR and Guideline 2 place an extensive list of requirements on a monitoring framework. The requirements converge on six core capabilities.

1

All customer behaviour in one assessment

Behaviour has to be assessed at customer level, across products and group entities, and across activities that only form a pattern when seen together. That means event monitoring rather than just transaction monitoring, taking non-transactional records in as well.

2

Detection reference points derived from the data

The guidelines ask for a profile of what is expected of a customer, rather than for assumed or arbitrary thresholds. Three baselines form that profile: the customer's own history, the peer group where it has explanatory value for that segment, and the counterparty network on the other side of the transaction.

3

Detection logic generated from the institution's own data

The framework has to fit this institution's risks and complexity. A model built on historic transactions, historic investigations and customer data is the best guarantee of covering the portfolio's risks, and it should produce detection logic that can be read and mapped onto the institution's risk assessment.

4

A complete record of what the framework did and why

Every alert is stored with the features and values that produced it, and every change to the logic is logged with its rationale and the date it took effect. This record needs to be readily accessible and understandable to staff, auditors and supervisors.

5

Performance measured on evidence

Performance measurement has to take place at multiple stages. This includes data quality checks, sampling and below-the-line testing, and measuring the produced alerts against known cases, with false and true positive rates tracked over time and drift monitored against the model's behaviour at validation.

6

The framework learns from what it finds

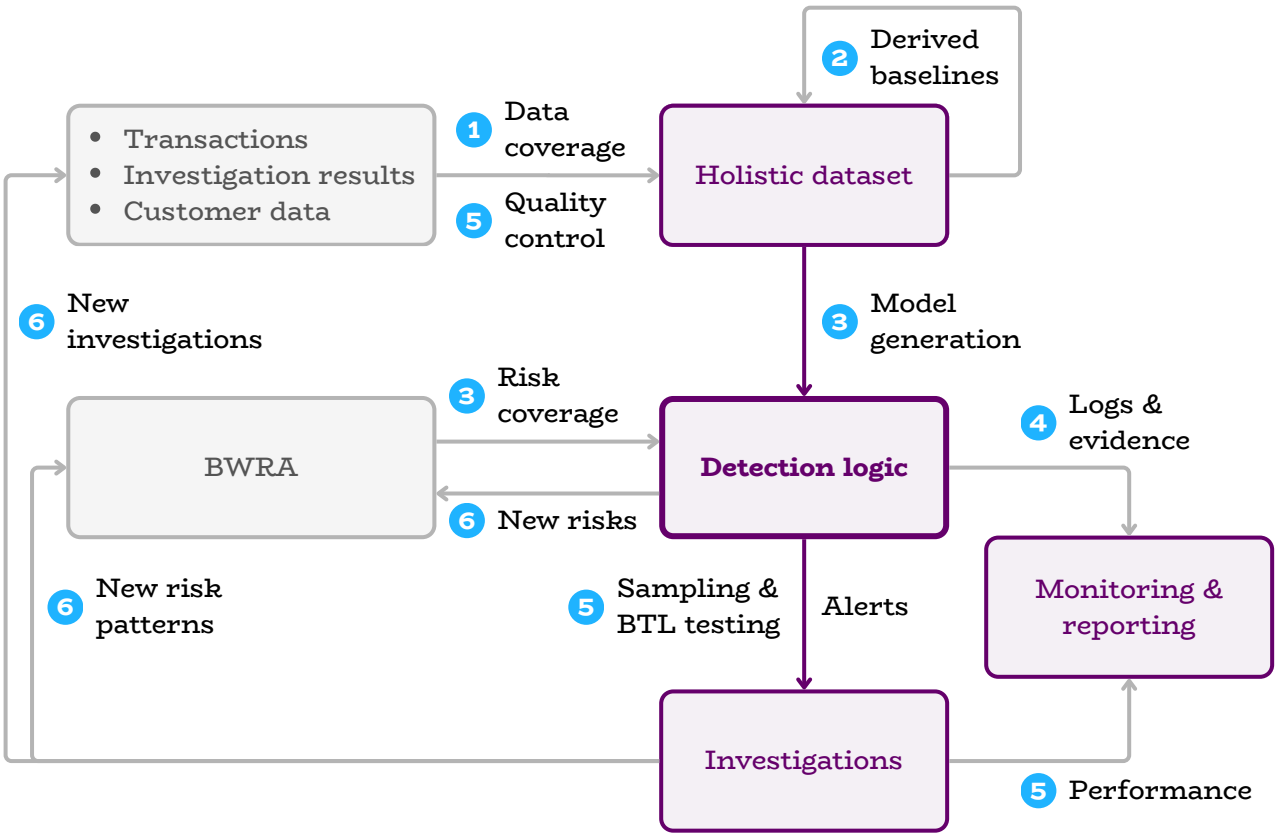
Keeping the framework current is an ongoing obligation. Investigation results, sampling results and new typologies feed the business-wide risk assessment and the available data for regenerating a next version of the detection logic.

The monitoring lifecycle

The **core process** runs from data to detection logic to alerts and investigations. The six capabilities sit at different points along it.

Detection logic is generated from the institution's own data and its business-wide risk assessment. Outcomes of risk coverage checks, sampling and performance assessments refine the logic further. The logic then runs, produces alerts, and those alerts are reviewed. What the reviews establish, together with what below-the-line testing shows, goes back into the risk assessment and into the data the next generation is built from.

Performance is measured throughout and monitored over time: on the quality of the data going in, on what the detection logic misses, and on the alerts it produces.



Part 1

1. All customer behaviour in one assessment
2. Detection reference points derived from the data
3. Detection logic generated from the institution's own data

Part 2

4. A complete record of what the framework did and why
5. Performance measured on evidence
6. The framework learns from what it finds

How Sygno addresses this

The Sygno platform generates transaction monitoring models from an institution's own data. Because the logic is generated rather than configured, the record of how it was built, what it does and why it changed comes out of the same process that produces the model.

Any data, any format, inside the client's environment

Transaction data, CDD attributes and non-transactional records come in from existing systems in whatever format they produce. Adopting the platform does not begin with a data cleaning project, and it runs inside the institution's own environment, so no customer data leaves it.

Individual, group and network in one assessment

A behavioural baseline is derived for each customer from that customer's own history. Peer group membership is tested as a variable rather than assumed, and counterparty and network characteristics enter on the same basis. Deviation is expressed as a distance from that baseline.

Explainable detection logic and complete audit logs

The output is an explicit ruleset that states which features drive each detection, readable by the people who operate it and traceable to the institution's risk assessment. Each alert carries the features and values that triggered it, and every change is versioned with its rationale and effective date.

Performance measurement built into the platform

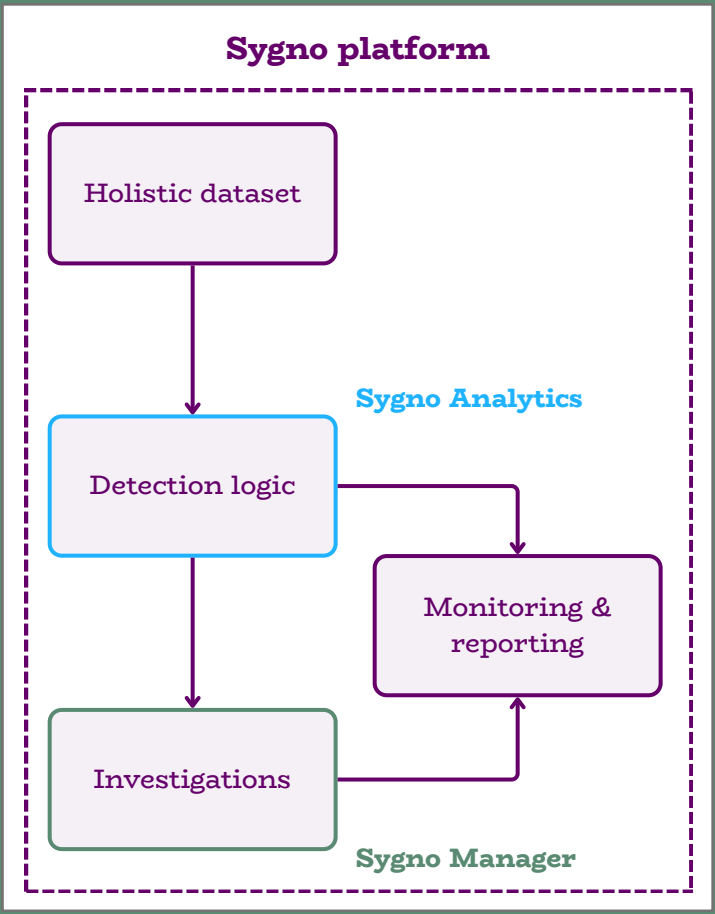
Detection is measured against known historic cases, false and true positive rates reported over time, model behaviour compared against validation, and data quality checked as part of the process. All of it sits in configurable dashboards that also generate reports for internal and external stakeholders.

Easy model regeneration that takes in what was learned

Modelling legitimate behaviour means anomalies surface without a pre-defined risk typology. Investigation outcomes, sampling results and changes to the risk assessment feed the next regeneration, which runs on current data without rebuilding the framework.

AMLA asks a great deal of the monitoring domain, and meeting it takes investment. Generating models from an institution's own data answers what Article 26 and Guideline 2 require, and at the same time changes what the framework finds: **more confirmed criminal activity** detected, and substantially **fewer false positives**. Monitoring and reporting take less effort, because the figures a supervisor asks for are the figures the platform already produces.

Sygno platform & modules



Sygno platform
Takes in the data, runs the monitoring and produces the reporting. Within the platform, the Analytics and Manager modules can run together (as a complete transaction monitoring engine) or separately alongside an existing setup.

Sygno Analytics
Generates the detection logic from the institution's own data. The output is an explicit ruleset that runs in the Sygno Manager or as a third-party model in another monitoring system.

Sygno Manager
Configurable case management system for the alerts the logic produces. Investigations are handled and recorded here, and their outcomes feed the next regeneration.

Timeline

Consultation on the draft guidelines: 3 June to 3 September 2026. Final guidelines expected in Q4 2026. AMLR applies from 10 July 2027.

The final text may differ from the draft, but the direction is unlikely to change. The guidelines leave little room for a framework that cannot do what they ask. Limitations have to be documented and mitigated, and they must not come from the institution's own design choices or from the systems it selected.

Obliged entities should already be assessing the gap and working out the options for closing it.

Convergence with the PSR

Para 34(a) asks obliged entities to build their monitoring framework on systems and processes already **required by other Union legislation**, naming Regulation (EU) 2023/1113 and the proposal for a regulation on payment services in the internal market. It is the only point in Guideline 2 where another instrument is named as a source of monitoring capability rather than as a boundary.

The two regulations serve different purposes. The PSR addresses fraud, and Guideline 2 addresses money laundering and terrorist financing. The capabilities they call for **overlap substantially**.

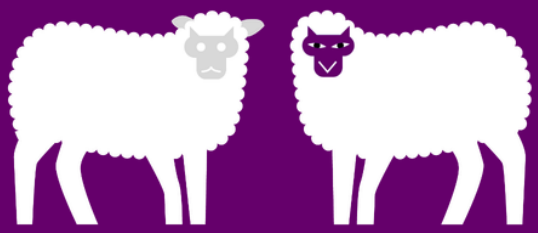
Both ground **monitoring in the customer's behavioural profile**: Article 83 PSR in behavioural characteristics typical of the payer and analysis of previous payment transactions, para 53 in a profile of what is expected of the customer.

Both point the institution towards its own data rather than towards shared or generic reference material. The PSR excludes behavioural characteristics from what payment service providers exchange between themselves, and paras 9 and 50 require the framework to be **commensurate with this institution's risks**, with no unassessed default settings.

Both require the institution to **account for its monitoring decisions**, the PSR through the reversal of the burden of proof and Guideline 2 through what has to be recorded, measured and explained about the framework, which Part 2 covers.

An institution that treats the two as separate projects **risks building the same capability twice**, since the underlying data, the behavioural baselines and the customer profiles are the same. What differs is the detection objective: fraud shows as a deviation from the customer's own baseline, while money laundering may be consistent with that history and deviate instead from what is expected of comparable peers or from what the counterparty relationship suggests. **That argues for looking at monitoring across both domains together, rather than running fraud and financial crime as siloed programmes.**

The PSR is at proposal stage and its final text may differ from the version referenced in the draft guidelines. Sygno's analysis of the transaction monitoring requirements in the PSR compromise text is set out in a separate PSR whitepaper.



About Sygno

Sygno provides automated model generation for transaction monitoring, helping financial institutions and other obliged entities detect financial crime more effectively and efficiently. By modelling the good, expected behaviour of customers, Sygno makes suspicious activity stand out, drastically reducing false positives while increasing the detection of unusual and suspicious transactions. Models are generated from your own data, are transparent and explainable to supervisors, and deploy into your existing transaction monitoring system without migration.
Know good, catch bad.

Contact



Sjoerd Slot

Chief Executive Officer

Sygno
www.sygno.com
getincontact@sygno.com
linkedin.com/in/sjoerdslot/

Zonnehof 40, 3811 ND Amersfoort
The Netherlands