Sygno

Transaction Monitoring under AMLA's Draft Guidelines

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

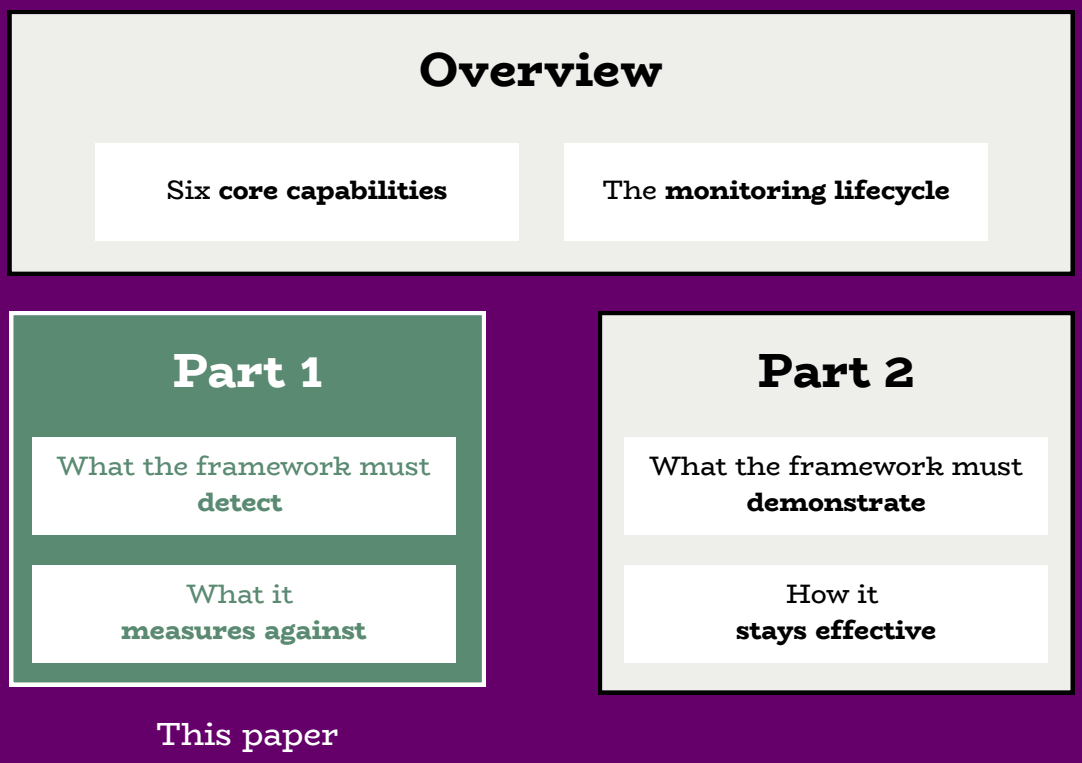
Whitepaper | August 2026

Status of this paper

This paper reflects the regulatory position as at August 2026. It is based on AMLA's consultation paper on draft Guidelines on ongoing monitoring of a business relationship under Article 26(5) of Regulation (EU) 2024/1624, published on 3 June 2026, with the consultation period closing on 3 September 2026 and final guidelines expected in Q4 2026. The guidelines are in draft form and may change following consultation. Where this paper refers to draft regulatory technical standards under Article 28(1) AMLR, those standards have completed consultation but have not yet been adopted by the Commission. References to AMLR articles are to the regulation as adopted and in force.

About this set of papers

This is one of a set of three papers covering AMLA's draft Guidelines on ongoing monitoring. The overview is an extended management summary of what the guidelines ask and what follows from it. Two detailed papers carry the analysis, provision by provision. This part covers what the framework must detect and what it measures against. Part 2 covers what the framework must demonstrate, and how it stays effective over time.



Introduction

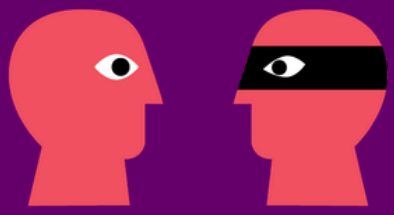
Article 26 AMLR requires obliged entities to conduct **ongoing monitoring of every business relationship.** That obligation has two components: keeping customer information up to date, and monitoring the transactions carried out during the relationship to establish that they remain consistent with the entity's knowledge of the customer, the customer's business activity and risk profile, and where relevant the origin and destination of funds. Article 26(5) mandated AMLA to issue guidelines on how that should be done.

The draft guidelines apply horizontally. They set out common expectations for all obliged entities in both the financial and non-financial sectors, and they are written around outcomes rather than prescribed methods. AMLA considered a prescriptive approach and rejected it, on the reasoning that detailed rules encourage adherence to enumerated steps in place of substantive risk assessment. What the guidelines specify is therefore what a framework must be capable of, and what an entity must be able to demonstrate about it.

One shift runs through the entire text. AMLA has adopted "transactions and activities" as standard wording throughout the guidelines, in place of the transaction-only language of Article 26 itself. The stated reason is the diversity of business models covered by AMLR, in which activity monitoring is central for certain categories of obliged entity. The wording has a legal anchor in Article 69(2) AMLR, which requires that a suspicion be based on, among other things, the size and nature of the transaction or activity, the methods and patterns of it, and the link between several transactions or activities. Where the guidelines expect both transactions and activities to be monitored, they expect both to be monitored equally.

For entities whose monitoring frameworks were built around transaction records, that shift changes what has to enter the system before any detection logic runs.

Scope of this paper. The focus is Guideline 2, on the transaction and activity monitoring framework. Guideline 1, on keeping customer documents, data and information up to date, is addressed only where it bears on monitoring: the events that trigger a customer information review, and the feedback from monitoring output into customer due diligence. Provisions on identity document re-collection, review frequency and suspension of services fall outside this scope.



The four themes

The requirements that Guideline 2 places on a monitoring framework group into four themes. Each takes a different question.

1

A single view of the customer

What the framework has to look at before it assesses anything. The guidelines widen the object of monitoring from transactions to activities, behaviours and events, and at the same time require the picture to be complete: across all products and services, drawing on group information, on data that is complete, accurate and timely. What falls outside the input cannot be detected downstream.

2

What deviation is measured against

The reference point that detection works from. The guidelines set out a chain running from verified customer due diligence information through to an expected behavioural profile for each customer, with peer groups permitted as a bounded supplement. The same chain runs in reverse: monitoring output has to inform the customer profile, the risk classification and, where relevant, the business-wide risk assessment.

3

Detecting across time and networks

What the framework has to be capable of finding. The guidelines are explicit that this includes risks visible only when transactions and activities are considered together over time: linked and repeated behaviour across accounts, customers, devices and other identifiers; value that is accumulated, split or moved; and network relationships that may conceal ownership, control or economic purpose.

4

Design and its limits

How the framework is arrived at. Proportionality appears here as a design requirement rather than a reduction in standard, and default settings may not be used without a documented assessment of their appropriateness. The theme closes with the requirement that the framework's own design must not stand in the way of compliance elsewhere.

Each theme sets out the requirements it places on an obliged entity, the provisions those requirements derive from, and the system properties they imply.

1 A single view of the customer

Monitoring can only assess what enters it. The first set of requirements in Guideline 2 concerns the input: what has to be brought into the framework, from where, and in what state. Three requirements follow from the relevant provisions.

A. Bring all relevant data together at customer level

B. Include non-transactional signals as detection input

C. Retain control over which data participates

Coverage, sources and timing

Where a business relationship covers more than one product or service, Article 26(1) AMLR requires customer due diligence to cover all of them. Para 34(c) carries that into the monitoring framework and adds the reason: to enable a **holistic understanding of the customer's behaviour**.

A framework that runs separate detection per product line covers every product while still producing several partial views of the customer. Where someone holds a payment account, a savings product and a credit facility, what matters may only be visible in how the three move relative to one another.

Article 26(1) extends the same logic across legal entity boundaries. Where group entities share customers, information about those other relationships has to be taken into account, whether or not the other entity is itself an obliged entity. The information has to be **available when the monitoring happens**, not assembled afterwards during an investigation.

Para 34(b) adds three conditions on the data itself. It must be **complete, accurate and timely**, drawn from internal sources and, where relevant, reliable independent ones. Completeness restates the coverage point above and accuracy is dealt with in Part 2. Timeliness constrains which monitoring approach is available at all. Data that reaches the framework a week after the event cannot support intervention before execution, whatever the detection logic is capable of.

Activities and events

Para 4 states that ongoing monitoring should not be limited to transaction monitoring but should also capture relevant **activities, behaviours and events**. The legal anchor is Article 69(2) AMLR, which bases suspicion on the nature of the transaction or activity, its methods and patterns, and the link between several transactions or activities.

Para 27(b) shows the range in practice: unusual transaction patterns, inconsistent behaviour, frequent and unexplained changes of professional service providers, and repeated or unusual changes in IP address or device location. Only the first is a transaction attribute. A framework built solely on transaction records has no representation of the others. The **system has to hold them** before detection can use them.

Para 44(b) requires analysis of behavioural patterns based on the customer's behaviour, relationships and transaction patterns over time. For an event to be **assessed over time**, it has to be recorded consistently: same field, same structure, same customer identifier, across the whole period.

Which data participates

Two provisions limit the input from the other direction. Para 10 applies proportionality to the amount and type of personal data processed for monitoring, following the GDPR principles of necessity and **data minimisation**. Para 94 requires analytical output to be governed so that **discriminatory outcomes are avoided**.

Both are decisions about fields, taken before the model is built. The framework has to **allow specific attributes to be excluded** from processing, and that exclusion has to hold through model construction rather than being applied as a filter on results. Note that excluding a field from the model does not make it unavailable to an investigation.

KEY PROVISIONS

- **Art. 26(1), second subparagraph, AMLR**: CDD measures cover all products and services where a relationship covers more than one
- **Art. 26(1), third subparagraph, AMLR**: Information on relationships with other group entities is taken into account, including where that entity is not itself an obliged entity
- **Art. 69(2), second subparagraph, AMLR**: Suspicion is based on the nature of the transaction or activity, its methods and patterns, and the link between several transactions or activities
- **Para 4**: Monitoring captures relevant activities, behaviours and events, not transactions alone

KEY PROVISIONS (continued)

- **Para 10**: Proportionality applies to the amount and type of personal data processed for monitoring
- **Para 27(b)**: Behavioural, activity-based and transactional anomalies are named as three categories of trigger event
- **Para 34(b)**: Framework relies on complete, accurate and timely data from internal and, where relevant, independent sources
- **Para 34(c)**: Framework covers all products and services to enable a holistic understanding of customer behaviour
- **Para 44(b)**: Analysis of behavioural patterns based on the customer's behaviour, relationships and transaction patterns over time
- **Para 94**: Analytical output is governed so as to avoid discriminatory outcomes

System implications

Requirement	Monitoring capability
A. Bring all relevant data together at customer level	Ingestion of records from other group entities, resolved to the same customer Ingestion and processing of varied source systems, formats and record types without loss of detail Feature computation at customer level, so behaviour across products contributes to a single assessment
B. Include non-transactional signals as detection input	Ingestion of non-transactional records: events, logins, device and channel attributes, changes in customer circumstances Detection on those attributes alongside transaction attributes, within one assessment Consistent retention of event history, so change in a non-transactional attribute is measurable over time
C. Retain control over which data participates	Field-level exclusion applied at model construction, not as a filter on output A record of which fields were available, used and excluded

2 What deviation is measured against

Detection on deviation needs something to deviate from. Guideline 2 sets out what that reference point is, how far it may be generalised, and what has to happen when monitoring finds something. Three requirements follow from the relevant provisions.

A. Record what is expected of each customer, and use it in the model

B. Let risk level drive the intensity of monitoring

C. Feed output back into CDD, risk classification and the business-wide risk assessment

The expected profile

Para 34(d) sets the detection criterion: the framework has to be capable of identifying transactions and activities that **materially deviate from expected behaviour** and require further assessment under Article 69(2) AMLR. What counts as expected is defined in para 53.

Customer profiles have to be based on verified customer due diligence information, and para 53 names what belongs in them: the purpose and intended nature of the business relationship, where relevant the expected transactions and envisaged activities, and the resulting **expected behavioural profile** of the customer.

The requirement is that the institution has recorded what it expects and that monitoring runs against it. An expectation that exists only as a form completed at onboarding is not part of the baseline detection works from. **Customer due diligence attributes have to enter the detection model** as variables, whether as risk classification, entity type, sector, purpose of the relationship or expected activity.

Para 54 permits reference or peer groups with an aggregated expected profile, on two conditions: **deviation from the group pattern is assessed in the broader context of the customer** rather than only at account level, and the absence of a deviation at peer-group level does not on its own dismiss risk indicators found at individual customer level. Similarly, para 55 adds that obliged entities should not solely rely on peer groups, particularly where customer behaviour is inherently heterogeneous. The provision asks that **peer groups support and not replace the understanding of the individual customer**, which leaves the individual profile as the reference point and the group profile as context around it.

Article 69(2) AMLR names the **characteristics of the customer and their counterparts** among the grounds on which a suspicion rests, which puts the other side of a transaction alongside the customer's own profile and the group profile as a source of context for the assessment.

Risk level as a parameter

Para 40 requires high-risk business relationships and transactions to receive **monitoring commensurate with their risk** and to be subject to enhanced scrutiny. It sets a limit in the same breath: increased intensity has to be targeted at areas of material risk and must not result in a disproportionate allocation of resources to lower-risk activities.

Para 41 lists what enhanced scrutiny can consist of. More targeted or intensified monitoring parameters, scenarios, risk indicators or analytical approaches. More frequent or in-depth reviews, including reviews covering an extended look-back period where that is relevant to assess patterns, links or cumulative risk indicators. Specific **controls adapted to the customer's activity and risk profile**.

Detection parameters that vary by risk level, and a look-back window that varies with them, are the practical form of both provisions.

The loop back

Three provisions describe the same movement. Para 6 requires **monitoring output to be assessed and used** to inform internal processes, including where appropriate the **update of customer due diligence information** and the customer's risk classification. Para 52 adds what follows when output indicates increased risk: risk-mitigating measures, which may include enhanced due diligence, and where the output indicates emerging or evolving risks, consideration of whether that has implications for the business-wide risk assessment. The analysis performed and the rationale for decisions taken have to be documented. Para 57 closes the sequence: where deviations or inconsistencies are identified, the customer's information and risk profile are reassessed and a decision taken on whether to submit a report under Article 69 AMLR.

Para 56 applies the same movement to the baseline itself. Profiles and peer group composition are reviewed and where necessary updated where monitoring output or other information indicates a material change in risk, behaviour or use of the service, **regardless of whether a periodic customer review is due.**

Article 23 of the draft RTS under Article 28(1) AMLR runs the same movement from the other end. Where an obliged entity reduces the frequency of customer identification updates in low-risk situations, it has to monitor the relationship to satisfy itself that circumstances have not changed, that no event has occurred requiring an update, and that no suspicious or unusual transactions or activities have been identified that are inconsistent with a low-risk relationship. **Anything monitoring finds therefore bears directly on whether the low-risk classification still holds**.

Taken together, these provisions ask for an **output that can carry** a decision. An alert identifier and a score are enough to open a case. Updating a risk classification or adjusting a customer profile takes a statement of what changed relative to what was expected, in a form that supports the decision and the record of it.

KEY PROVISIONS

- **Art. 23, draft RTS under Art. 28(1) AMLR**: Reduced frequency of customer identification updates requires monitoring to confirm that circumstances are unchanged and no inconsistent activity has been identified
- **Art. 69(2), second subparagraph, AMLR**: Suspicion is based on the characteristics of the customer and their counterparts, alongside the consistency of the transaction or activity with the information obtained under Chapter III including the customer's risk profile
- **Para 6**: Monitoring output assessed and used to inform internal processes, including CDD updates and risk classification
- **Para 34(d)**: Framework capable of identifying transactions and activities that materially deviate from expected behaviour and require further assessment under Article 69(2) AMLR
- **Para 40**: High-risk relationships receive monitoring commensurate with risk, targeted at material risk
- **Para 41**: Enhanced scrutiny may include intensified parameters, scenarios and analytical approaches, and an extended look-back period
- **Para 52**: Output indicating increased risk triggers mitigating measures; output indicating emerging risk is weighed against the business-wide risk assessment; analysis and rationale documented
- **Para 53**: Customer profiles based on verified CDD information, including the resulting expected behavioural profile; monitoring calibrated to that baseline
- **Para 54**: Peer groups permitted; deviation assessed in the context of the individual customer; absence of group-level deviation does not dismiss individual indicators
- **Para 55**: Peer groups support rather than replace understanding of the individual customer, and are not to be relied on where behaviour is heterogeneous
- **Para 56**: Profiles and peer group composition reviewed and updated where monitoring output indicates material change, regardless of the periodic review cycle
- **Para 57**: Deviations trigger reassessment of customer information and risk profile, and a decision on reporting under Article 69 AMLR

System implications	
Requirement	**Monitoring capability**
A. Record what is expected of each customer, and use it in the model	CDD attributes available as model variables alongside behavioural features Peer group treated as a candidate variable, selected on predictive value per segment rather than applied uniformly Individual and peer-group deviation both assessed, with neither suppressing the other Counterparty network available when assessing a transaction against the customer's own baseline
B. Let risk level drive the intensity of monitoring	Detection parameters that differ by customer risk classification Configurable look-back window, extendable for higher-risk relationships Detection on lower-risk activity that surfaces unusual behaviour without generating volume (false positives) that pulls resources away from material risk
C. Feed output back into CDD, risk classification and the business-wide risk assessment	Profiles and group composition revisable on monitoring output, outside the periodic review cycle Output stating which expectation was departed from and by how much, in a form that supports a CDD decision Retained record of the analysis and the reasoning behind each decision

3 Detecting across time and networks

A transaction that clears every threshold on its own can still be part of something that does not, and a party that looks unremarkable in isolation can look different once its connections are visible. Guideline 2 requires the framework to find what only becomes apparent when transactions, activities and parties are placed alongside one another. Two requirements follow from the relevant provisions.

A. Detect patterns across transactions and activities, including value that is accumulated, split or moved

B. Detect connections between accounts, customers, devices and counterparties

Patterns across transactions and activities

Para 44 requires the framework to be capable of **detecting risks that only emerge when transactions and activities are considered together over time**, rather than in isolation. Article 69(2) AMLR carries the same idea into the reporting obligation, basing suspicion partly on the methods and patterns of a transaction or activity and on the link between several of them.

Para 44(d) gives the clearest case. The framework has to recognise situations where individual transactions and activities may appear **low-risk on their own but form concerning patterns or behaviours over time**, including cases where value is accumulated, split, or transferred across multiple transactions and activities.

Detection that evaluates each transaction against a threshold cannot reach that. Splitting a payment into amounts below any single limit leaves nothing for a per-transaction test to find, because each part passes on its own and the pattern exists only in the set. **The unit of assessment has to be a sequence over a window rather than the individual record**.

Para 44(a) sets the scope of that aggregation: linked, repeated or **aggregated behaviour across and within accounts, customers, devices, wallets or other identifiers**. Aggregating within one account is the narrowest reading of the provision and the one most existing systems already do. The provision reaches further, to behaviour that is the same customer's but spread across accounts, and to identifiers that link records the customer file does not connect.

Para 70 places that analysis inside **post-transaction monitoring**. Where obliged entities have the ability to analyse transactions and activities after they have been carried out, including, where relevant, on an aggregated or behavioural basis, that analysis has to form part of post-transaction and post-activity monitoring. Aggregation over time is therefore not conditional on being able to intervene before execution, and an institution that monitors only in real time and only per transaction is not meeting para 44 by pointing at what its real-time layer can do.

Para 39 extends the same analysis to complex products, services and business models, including correspondent banking, trade finance, and investment and wealth management. Monitoring there should not focus solely on individual transactions and activities but may also involve the **analysis of aggregated flows, activity patterns, documentary information or changes in the form or structure of value**. Value that moves between instruments, asset classes or legal wrappers is only traceable if the framework can follow it across those changes.

Connections between parties

Para 44(c) requires the framework to recognise **network relationships or behavioural patterns** that may indicate attempts to conceal ownership, control or the economic purpose of an activity. Concealment of that kind shows in how parties relate to one another, and in flows that make sense only when the relationship between the parties is known.

Para 34(e) lists where those connections can be found: **through intermediaries, ownership or control structures, counterparties, assets or transaction patterns**. The provision is written for risks of non-implementation or evasion of targeted financial sanctions, but what it asks the framework to find is not specific to sanctions. The same structures and counterparty relationships that hide a sanctioned party can hide the origin of funds or the person a transaction is really for.

Both provisions place **counterparty and structural data inside the detection input** rather than in the investigation that follows an alert. A framework that holds only the customer side of each transaction has no material to find these patterns in.

KEY PROVISIONS

- **Art. 69(2), second subparagraph, AMLR**: Suspicion is based partly on the methods and patterns of a transaction or activity and on the link between several transactions or activities
- **Para 34(e)**: Identification of patterns, behaviours or linkages through intermediaries, ownership or control structures, counterparties, assets or transaction patterns
- **Para 39**: For complex products and business models, analysis of aggregated flows, activity patterns, documentary information or changes in the form or structure of value
- **Para 44**: Framework capable of detecting risks that emerge only when transactions and activities are considered together over time
- **Para 44(a)**: Identification of linked, repeated or aggregated behaviour across and within accounts, customers, devices, wallets or other identifiers
- **Para 44(c)**: Recognition of network relationships or behavioural patterns indicating attempts to conceal ownership, control or economic purpose
- **Para 44(d)**: Recognition of transactions that appear low-risk individually but form patterns over time, including accumulation, splitting or transfer of value
- **Para 70**: Aggregated and behavioural analysis forms part of post-transaction and post-activity monitoring, to identify unusual patterns, linkages or cumulative risk indicators

System implications

Requirement	Monitoring capability
A. Detect patterns across transactions and activities, including value that is accumulated, split or moved	Assessment over a sequence of transactions within a window Assessment in real time and over completed history Aggregation across the accounts, products and instruments held by the same customer, including where value changes form Detection of accumulation, splitting and onward transfer of value as patterns in their own right
B. Detect connections between accounts, customers, devices and counterparties	Resolution of customers, accounts, devices, wallets and other identifiers to a common entity Counterparty and ownership structure data held as detection input, not only as investigation material Relationships between parties assessable as a structure

4 Design and its limits

The first three themes describe what a framework has to find. This one concerns how it is arrived at, and what has to be true of it before it goes into use. Two requirements follow from the relevant provisions.

A. Derive the detection logic from this institution's own risk profile

B. Keep the framework's own design from limiting compliance elsewhere

Built for this institution

Para 9 requires the monitoring framework to be designed and implemented in a manner commensurate to the nature, risks and complexity of their business, as well as the size of the obliged entity. AMLA states in the background section of the consultation paper that proportionality should not be understood as implying lower or weaker standards for smaller obliged entities, and that size is only one factor alongside overall risk profile, complexity, scale and business model.

Para 34(f) adds what the framework has to achieve at that point: it is designed to be effective, at the point of implementation, in **addressing the risks identified in the obliged entity's business-wide risk assessment**. The framework therefore has to be effective against those risks when it goes live, not at some later point of tuning.

Para 48 sets out what has to be defined. Rules, scenarios, thresholds and models or behavioural baselines have to be **clearly defined and capable of detecting the relevant risks**, taking into account relevant typologies and the general principles in para 34.

Para 49 adds a condition on every design choice made along the way. When designing and adjusting the framework, obliged entities should consider the potential **impact of their choices on both detection capability and the risk of undetected activity**. Detection capability shows itself in what the framework produces. The risk of undetected activity does not, which makes it the side of the balance an institution has to go looking for. Establishing that risk means testing against activity the framework did not flag, which Part 2 covers.

Para 50 addresses what happens when the logic comes from outside. Where obliged entities rely on pre-configured or externally developed monitoring tools, they have to understand the appropriate use of those tools, review and assess the suitability of the default settings, and calibrate them. Default settings should not be used without a documented assessment of their appropriateness. Read alongside para 9, that assessment has to establish that settings arrived at for a general case are appropriate for this institution's risk profile, customer base and product mix. An institution that cannot make that case has to calibrate the settings until it can, or derive the logic itself. **While the provision ultimately does permit the use of pre-configured logic, it makes the institution carry the burden of showing it fits.**

No self-imposed limits

Para 58 sets the general rule that **ongoing monitoring is performed on a continuous basis** throughout the business relationship.

Paras 66 and 73 run parallel, applied to **pre-transaction and post-transaction monitoring** respectively. Both state that limitations must not create gaps in the ability to identify, assess and escalate risks. Both add that those limitations should not arise from, or be reinforced by, the design of products, services or business practices, which should support the effective application of monitoring measures and should not unduly restrict it.

Both paragraphs close by narrowing what can be offered as justification. Legal or technical constraints should not be used to justify the absence of monitoring where the obliged entity is in a position to assess or intervene. Whether a monitoring system an institution has chosen and operates counts as a constraint beyond its control is not addressed in the guidelines. But it is difficult to argue that it does. **A limitation by a vendor the institution chose, and can replace, is not the same thing as a constraint imposed on it from outside.**

What the provision does settle is that the framework's own design cannot become the reason a requirement elsewhere goes unmet. **The capabilities set out in the first three themes have to be achievable together, in one coherent framework.**

KEY PROVISIONS

- **Para 9**: Framework designed and implemented commensurate to the nature, risks and complexity of the business and the size of the obliged entity, with size only one factor among several
- **Para 34(f)**: Framework designed to be effective, at the point of implementation, in addressing the risks identified in the business-wide risk assessment
- **Para 48**: Rules, scenarios, thresholds and models or behavioural baselines clearly defined and capable of detecting the relevant risks

KEY PROVISIONS (continued)

- **Para 49**: Design and adjustment weigh the impact of each choice on both detection capability and the risk of undetected activity
- **Para 50**: Default settings of pre-configured or externally developed tools not used without a documented assessment of their appropriateness
- **Para 58**: Ongoing monitoring performed on a continuous basis throughout the business relationship
- **Para 66**: Limitations on pre-transaction and real-time monitoring must not create gaps, must not arise from the design of products, services or business practices, and legal or technical constraints do not justify the absence of monitoring where the entity can assess or intervene
- **Para 73**: The same as para 66, applied to post-transaction and post-activity monitoring

System implications

Requirement	Monitoring capability
A. Derive the detection logic from this institution's own risk profile	Rules, scenarios, thresholds and behavioural baselines clearly defined and readable, white-box rather than black-box Detection logic generated from the institution's own transaction and customer data Detection logic that can be verified to cover the risks in the business-wide risk assessment, before the framework goes into use Evidence of what the design detects and of what it leaves undetected Evidence that the detection logic fits this institution's risk profile, customer base and product mix
B. Keep the framework's own design from limiting compliance elsewhere	Continuous operation across the relationship rather than periodic batch assessment A combination of tooling and capabilities that leaves no technical gaps in the monitoring requirements

From theory to practice

This paper has looked at **what the monitoring framework must detect** and **what it measures against**. Guideline 2 approaches that through four themes: what enters the framework, what deviation is measured against, what only becomes visible across time and connections, and how the detection logic is arrived at. The requirements those themes place on an institution converge on **three core capabilities**.

1

All customer behaviour in one assessment

Behaviour has to be assessed at customer level, across products, across group entities, and across transactions and activities that only form a pattern when seen together. That means taking in records from different source systems and formats without losing detail, holding non-transactional events with the same structure as transactions, resolving accounts, devices and other identifiers to one customer, and assessing over a window rather than per record.

2

Detection reference points derived from the data

What the guidelines ask for is a profile of what is expected of this customer, with detection measured against it. Three reference points do that work together: the customer's own history, the peer group where the group has predictive value for that segment, and the counterparty on the other side of the transaction. The same amount moving between the same two accounts means different things depending on who those parties are and what the customer has done before, and an assessment that cannot see all three is missing crucial information to monitor in a compliant manner.

3

Detection logic generated from the institution's own data

Default settings cannot be used without a documented assessment of whether they suit this institution, and the framework has to be commensurate with its risks and complexity. Logic derived from the institution's own transaction and customer data and from its business-wide risk assessment answers that directly, and produces an explicit ruleset rather than a score without provenance. That ruleset can be read, validated against the risks the institution has identified, and shown to a supervisor.

Together these three determine whether a monitoring framework meets what Article 26 and Guideline 2 ask of it. They belong at the centre of the decisions an institution takes on the way there: how to **design** the framework, which tooling and vendors to **select**, and how to **account** for those choices towards the supervisor.

How Sygno addresses this

The Sygno platform generates transaction monitoring models from an institution's own data, in line with AMLA requirements. The resulting detection logic is fit-for-purpose and specific to that institution, and explainable to both technical and compliance teams.

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

The generation process takes in transaction data, customer due diligence attributes and non-transactional records from the institution's existing systems, in whatever formats those systems produce. The platform imposes no requirements on how that data is structured, so adopting it does not begin with a data cleaning project. It runs within the institution's own environment, and no customer data leaves it at any stage of generation or operation.

Individual, group and network in one assessment

Sygno derives a behavioural baseline for each customer from that customer's own history, and tests peer group membership as a variable rather than assuming it. Where a group has explanatory value for a segment it is retained; where it has none it is not. Counterparty and network characteristics enter the assessment on the same basis. The baseline is built from a combination of characteristics rather than a single measure, and deviation is expressed as a distance from it. The same behaviour reads differently depending on the customer, the group and the party on the other side.

Explainable and compliant detection logic

The output of the generation process is an explicit and understandable ruleset. It states which features drive each detection, in a form that can be read by the people who operate the framework and checked against the risks in the institution's business-wide risk assessment. Where an institution has to account for its detection logic, it is accounting for logic derived from its own portfolio rather than for settings adopted from elsewhere.

Runs alongside an existing setup, or standalone

Sygno can replace an existing monitoring setup, but more often it runs alongside an existing one. The generated ruleset is then run inside the existing system, which lets an institution meet the AMLR monitoring requirements without an immediate technical and operational overhaul.

Keeping a framework effective after it goes live raises further questions: how effectiveness is measured and what may be offered as evidence of it, how models are validated and revalidated, how performance degradation is detected, what has to be explained to a supervisor and to the institution's own staff, and what an institution has to know about the data and the tools it depends on. Those are covered in **Part 2**.

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