

Audit-ready and still missing the risks

Why the AMLR requires more than legally defensible standard solutions.

Focus Paper · Discussion paper · Version 1.0
Sven Eisermann · 14 October 2026 · English version

The AMLR requires institutions to exercise their own judgement on risk. An approach to implementation that primarily seeks standard solutions as immune to challenge as possible may fail to achieve this objective.

It is easy to win agreement with the proposition that anti-money laundering must go beyond formalities. Hardly anyone would describe their approach as ignoring risks and merely working through regulatory requirements. The natural response is to point to the institution's risk assessment, a customer risk-scoring model with tailored weightings and graduated sets of measures. After all, the necessary tools are in place.

This is precisely where a misunderstanding can arise. An institution may have all these tools and still replace significant parts of its risk assessment with standardised and formalised routines. The factors come from recognised sources, their weightings have been adjusted and the risk categories are defined. What may still be missing is a sound understanding of how its own business could actually be misused.

Another reference to the risk-based approach is unlikely to remedy this weakness. The first step would be to establish what the term is understood to mean. As long as selecting predefined factors and converting them into a score counts as sufficient evidence, expectations of institutions' own risk management remain remarkably low.

This is a fundamental problem for AMLR implementation. It also concerns legal advisers, who help shape how the framework and its practical implications are understood.

'Reading' the full legal mandate

AMLR implementation requires a careful analysis of the legal requirements. Without it, processes cannot be reliably designed or responsibilities assigned. But anyone who looks primarily for explicitly specified data, documents and procedural steps risks overlooking a substantial part of the regulatory mandate.

Articles 9, 10 and 20 AMLR link risk management, institutions' own risk identification and individual customer risk assessment to the appropriateness of the measures. Appropriateness goes beyond formal compliance. Measures must be tailored to the identified risks, capable of managing them effectively and proportionate in nature and extent. Obligated entities must also be able to justify their institution-specific conclusions and decisions to their supervisor.¹

This creates a task that cannot be completed simply by cataloguing individual obligations. A measure must be *understood in its context*. Its purpose, the understanding it is expected to produce and the decisions that should follow are as much part of legal interpretation as its wording.

From a legal perspective in particular, a requirements list should not be considered sufficient simply because it is as comprehensive as possible. Reducing a provision to its expressly specified individual steps while disregarding the duty to exercise one's own judgement does not amount to particularly cautious implementation. It interprets the mandate too narrowly.

None of this means invoking the purpose of the law to override specific requirements. Nor does the general objective of prevention justify any additional requirement one might choose to impose. What is needed is an interpretation that brings together binding obligations, the institution's own judgement and proportionality.

¹ Regulation (EU) 2024/1624, Article 9(1), Article 10(1) and (2), and Article 20(2) and (4).

The duty to manage risk is not an invention of the AMLR. Section 4 of the German Money Laundering Act (GwG) already requires effective risk management appropriate to the institution's business activities.² The new Regulation should therefore prompt a critical review of existing implementation. A long-standing requirement is not better fulfilled by translating it once again into a larger collection of standard rules.

A tailored score is not yet an institution's own risk identification

One objection to this criticism is that institutions do apply official risk factors to their own circumstances. They do not adopt everything unchanged. They assess relevance, determine weightings and take their business models into account. Their models therefore also differ from one another.

This is a useful part of the work. But it should not be treated as evidence of more than it actually establishes. Assessing which known factors fit the business can support an institution's own investigation of its actual exposure. It does not replace that investigation.

The AMLR expressly treats the risk variables and risk factors in Annexes I to III as non-exhaustive.³ Anyone who nevertheless stays exclusively within that framework must at least be able to explain why the factors it captures are sufficient for the institution's own business. It is also possible to conclude that particular listed indicators are not relevant to the risks of that business.

Tailoring someone else's catalogue of risks does not, by itself, demonstrate that an institution has independently (and comprehensively) identified its own risks.

Independent does not mean original. A bank does not have to invent new money laundering methods or necessarily reach different conclusions from its competitors. But it should be able to explain its exposure by reference to its own specific business. This requires an understanding of its customers, the services and products it offers, how they are actually used and where vulnerabilities may lie.

A hypothetical example illustrates the difference. A bank mainly serves domestic companies. Country and sector risks have been examined, and its customer risk scoring is clearly documented. Certain interconnected companies, however, receive funds across several accounts before pooling and transferring them onwards. Monitoring treats each account separately.

This arrangement may be entirely legitimate from a commercial perspective. It may also warrant a closer examination of the connections between payments and a review of the suitability of existing monitoring. A correct assessment of country risk as low does not establish whether examining the accounts in isolation leaves a material detection gap.

The risk assessment would need to examine a possible mechanism of misuse. An additional score is only useful once it is understood what that score is intended to represent and which decision should follow from it.

For its material risks, an institution should therefore be able to explain how misuse might work, why its own business would be vulnerable and how the proposed measures are intended to address that vulnerability. The origin of the factors and the mathematical logic of the score provide only part of the answer.

² Section 4(1) of the German Money Laundering Act (GwG).

³ Regulation (EU) 2024/1624, the opening sentence of each of Annexes I, II and III; see also Article 10(1) and Article 20(2).

Hard to challenge does not mean appropriate

Relying on recognised factors and standards is understandable. They provide reference points on which decisions can be based. An institution's own findings, by contrast, require explanation and may be challenged. A different weighting, the decision not to request a customary additional document or a control that departs from the standard all need justification.

Where such decisions take considerably more effort to defend than adopting an industry solution unchanged, a problematic incentive arises. The institution increasingly designs its implementation around whatever appears least open to challenge.

The result can be an extensive and costly compliance organisation whose particular strength lies in demonstrating conformity with its own procedures. That is by no means insignificant. It is simply not enough to establish the quality (and effectiveness) of its risk management.

The aim of minimising effort also deserves closer examination. Cost-effectiveness is legitimate. It becomes problematic when the required level of effort is to be fixed before the risks have been adequately examined. The desired minimum then determines the analysis, even though the analysis should determine which measures are necessary.

There need not be any reduction in forms or procedural steps. The avoidance may lie elsewhere. Investigating risks independently takes time, requires expertise and can produce uncomfortable findings. A standardised procedure is easier to manage organisationally.

Legal assessment carries a particular responsibility here. Anyone offering standard answers designed to withstand challenge without examining their substantive suitability for the relevant risk may reinforce this misdirection. Referring to common practice does not relieve an institution of the need to exercise its own judgement.

Audit-readiness should follow from a sound risk assessment. It becomes the wrong objective when it is achieved primarily by avoiding independent decisions wherever possible or replacing them with standards.

The supposed gap in the rules

Against this background, calls for further guidance and more detailed AMLR requirements take on a different significance. Clearer terminology, consistent requirements and reliable supervisory expectations are necessary. But they do not create an entitlement to a ready-made answer for every operational situation that can be transferred into the institution's own practice without individual adaptation.

Genuine legal uncertainty and a duty to exercise one's own judgement are different things. The former may require authoritative clarification. The latter must be fulfilled by the obliged entities themselves. An internal decision that has not yet been made does not become a legal uncertainty simply because an industry standard would make it easier.

Saying that there is no specific rule for a particular situation therefore tells us little on its own. What matters is whether legal guidance is genuinely missing, or whether a professionally reasoned decision is possible and necessary within the existing framework. The intention behind a provision and its purpose or objective provide a central basis for that assessment.

Legislators can set general standards and impose specific obligations. These generally constitute minimum requirements that follow a rules-based approach. They cannot, however, anticipate every possible form of misuse and the appropriate countermeasures for every business model. Anyone waiting for such completeness is placing expectations on the framework that are difficult to reconcile with taking responsibility for one's own risk management.

AMLA also rejects a mechanical approach to implementation. In its Final Report of 30 September 2026 on the final draft CDD RTS, it explains that excessive detail should be avoided and that the provisions should not be understood as checklist obligations. Their application should be proportionate, risk-based and related to the obliged entity's particular circumstances. This explanation concerns a final technical draft and must be distinguished from the adoption of a binding legal act.⁴ The move away from mechanical implementation described in the report underlines the responsibility for institution-specific decisions. Examples and guidance can provide a starting point. They are no substitute for either the institution's own risk assessment or compliance with binding requirements.

The desire for harmonisation thus sits alongside responsibility for an institution's own judgement on risk. Standards can support that judgement and improve its quality. If they are made a prerequisite for every decision, however, they ultimately serve to shift responsibility elsewhere.

For legal advisers, this means explaining where room for judgement exists. Treating every missing detail as an implementation problem can easily suggest that proper prevention starts only once the next clarification arrives. In many areas, the task is precisely to reach a defensible conclusion without a fully prescribed solution.

Understanding customers rather than completing files

The same narrowing of focus can occur in the KYC process when formal data collection and completeness become the main criteria of quality.

A customer file may contain every required item of information and still fail to provide a coherent picture of the business relationship. The nature of the business, beneficial owners and purpose of the account are documented. It remains unclear whether the expected payment flows fit that picture, which arrangements would need explanation and which risks arise from them.

The substantive requirement already goes further under the existing GwG. Section 10 GwG covers both assessing the purpose of the business relationship and whether transactions are consistent with the institution's knowledge of the customer.⁵

In this sense, UYC, or *Understand Your Customer*, can provide a useful emphasis that goes beyond formal knowledge of the customer (KYC). The term is not intended to create a new category of obligation or an additional questionnaire. Here, it describes the quality of understanding that should result from assessing the available information.

This includes a reasoned understanding of the customer's business or circumstances and expected behaviour. Only on that basis can an institution assess which deviations matter and which measures make a useful contribution. Findings from monitoring must, in turn, be capable of changing that understanding of the customer.

More information does not automatically mean less risk. Additional evidence of the source of funds may initially reduce uncertainty. It may equally reveal inconsistencies that justify a higher risk assessment. A higher risk assessment must therefore also be considered a possible outcome. The review must not focus solely on rebutting the specific indication of risk.

A document creates value through its assessment and the consequences drawn from it. Its mere presence in the file does not mitigate risk.

Nor should a low score obscure the fact that important connections have not been understood. An inadequate information base and a well-founded assessment of low risk must remain distinguishable.

⁴ AMLA, Final Report on the draft CDD RTS under Article 28(1) AMLR, 30 September 2026, pp. 47–48.

⁵ Section 10(1), points 3 and 5, of the German Money Laundering Act (GwG).

Risk must determine the measure

Even sound risk identification can lose its value if subsequent handling falls back into rigid routines.

An overall score condenses different pieces of information. This is useful for prioritisation. When selecting specific measures, however, the differences lost in that aggregation may be precisely the ones that matter.

An opaque ownership structure requires a different response from payment activity that cannot be explained by the stated business model. Both customers may fall into the same risk category. An identical package of additional documents will not necessarily address these different problems.

The level of risk primarily influences the intensity of the response. The nature of that risk determines which measures are suitable. Reducing these two dimensions to a single category inevitably leaves risk management imprecise.

The AMLR does not equate enhanced due diligence with a single package to be applied indiscriminately. Article 34 addresses both higher risks specified in law and those identified by the institution itself, and requires proportionate enhancement. Specific mandatory measures must still be observed.⁶

Greater differentiation within the higher-risk range can help keep relevant differences visible. An internal scale might, for example, distinguish Low, Standard, High-low, High and High-high. Alongside a lower-risk range and a standard range, it would provide several gradations of genuinely higher risk and allow a more risk-differentiated response.

This would be a possible conceptual design, not a scale prescribed by regulation. It would imply neither equally wide risk bands nor fixed proportions of customers. Its value would have to be demonstrated by a more precise allocation of resources and measures.

Five rigid packages would, however, be little improvement on three. The additional differentiation needs to be linked to the relevant risk drivers. Reliable core processes can be combined with appropriate modules of measures and reasoned adjustments. Comparable cases can be handled consistently, provided material differences are not lost.

This is also where a risk-focused perspective may prove useful. The term is not intended to replace the regulatory risk-based approach (RBA). It is a reminder that risk must remain decisive throughout the process. Calculating it once and then simply working through the assigned procedure is not enough.

This includes the deliberate allocation of scarce resources. The FATF expressly connects the risk-based approach with concentrating on higher risks and allowing simplified measures where risks are lower.⁷

Distributing additional checks as evenly as possible across all risk levels can work against this principle. Work that produces no corresponding improvement in understanding or control ties up capacity that is then unavailable for material concerns. Anyone designing effective prevention must therefore also be able to explain where additional work fails to serve its purpose.

⁶ Regulation (EU) 2024/1624, Article 34(1), (3) and (4), read together with Article 20(2).

⁷ FATF, Guidance for a Risk-Based Approach – The Banking Sector, October 2014, particularly the conceptual explanation on the publication page.

Legal advice must enable decisions

This approach to implementation requires support from management, supervisors and auditors. If every departure from a standard attracts particular scrutiny while its uncritical adoption requires little justification, defensive decisions should come as no surprise.

In its 2021 guidance on risk-based supervision, the FATF already called for a move away from box-ticking and described the change in supervisory culture that this requires.⁸

When reviewing an institution, auditors should therefore examine not only whether a measure was carried out, but also whether it was suitable. A complete file calls for a different assessment from a sound judgement on risk. The two may coincide, but they need not.

Independent judgement does not mean less accountability. The standards for its justification are demanding. Assumptions must be identifiable, the limits of available knowledge disclosed and decisions reviewed when new information emerges. A transparent process provides the framework within which different circumstances can legitimately produce different outcomes.

Legal advice on AML should foster precisely this capability. Anyone explaining what the AMLR requires must also explain which decisions it assigns to obliged entities and how those decisions can be made on a legally sound basis and, above all, documented.

Advice that primarily identifies new individual requirements and criticises the lack of detail can instead reinforce the misunderstanding. Practitioners then wait for further instructions, although part of their task already consists of reaching a reasoned conclusion themselves.

The criticism therefore concerns a narrowing of professional perspective, not legal rigour. Risk management needs legal knowledge. But implementing AML law also requires legal advisers to understand the activity they seek to regulate.

A compliance architecture designed to be as immune to challenge as possible must not replace a serious examination of the actual risk of misuse.

Use the gap

When next revising the risk assessment, it is worth setting aside time for an investigation whose outcome has not already been decided. A useful starting point would be a material business area, examining how it actually operates together with the people who know its customers, products and operational problems through their day-to-day work. Actual business transactions, unusual cases and difficulties encountered in handling them may yield more insight than another refinement of the existing catalogue of factors.

Such an investigation requires openness to findings that do not fit the existing picture. A familiar process may prove more vulnerable than assumed. Conversely, a factor previously given substantial weight may be less informative about the actual exposure than expected. Both findings should be allowed to have consequences. Anyone merely seeking confirmation of the previous assessment will learn little, even from an elaborate analysis. The focus should be on realistic possibilities of misuse and understandable connections, not on the most dramatic scenarios imaginable.

⁸ FATF, Guidance on Risk-Based Supervision, 4 March 2021, particularly the explanation of the change in supervisory culture on the publication page.

This work takes time. Some of that time can be recovered by taking a more targeted approach to adopting and maintaining external requirements and standards. Binding requirements must still be met, and published risk factors must be carefully assessed for their significance to the institution's own business. But not every indicator should mechanically produce an additional model factor, a new data field or another review process. The specific purpose of that effort should be clear. Simply assuming that someone, somewhere, probably expects it is not a sound justification.

Existing procedures deserve the same scrutiny. Duplicate checks, rarely used information and routinely requested evidence should be reviewed for their actual contribution. Where work can be removed within the limits of the law, capacity becomes available for more demanding professional analysis. This is not a blanket cost-cutting programme. A serious investigation of risk may require additional measures elsewhere. Its value lies in making the reallocation of effort to where it is needed more readily justifiable.

The investigation must then lead to decisions. Its findings should inform control design, customer assessment and the prioritisation of further work. Unresolved questions should remain visible, with an assigned owner and a specific plan for resolving them. There should also be a clear basis for assessing later whether an adjustment has actually improved anything. Management must allow time for this work and be prepared to accept findings that challenge previous assumptions or established practices.

It is in this sense that the supposed gap can be used. What is meant is the room to design a reasoned, institution-specific approach within binding requirements. Making use of that room requires expertise, curiosity and a willingness to stand behind a decision that cannot be justified solely by reference to an industry standard.

We should devote more of the time currently spent covering every perceived expectation as a precaution to understanding what our own business actually needs. That is precisely why the available room for judgement is worth using.

This article is a discussion paper on AMLR implementation, reflecting the position as at 14 October 2026. It describes possible misdirection in implementation and makes no claim to provide empirical findings for the industry or the legal profession as a whole.

The AMLR generally applies from 10 July 2027. References to the existing GwG provide context for the pre-existing risk management mandate. The AMLA report cited explains a final technical draft and is not treated as an already adopted legal act.

Sven Eisermann · AML/CTF.eu

© 2026 Sven Eisermann. The views expressed are the author's professional position and are intended to provide general context. They do not replace an assessment of the specific circumstances of an individual case and do not constitute legal advice.