ACUMINOR

Acuminor's official response to AMLA Draft Guidelines on the Business-wide risk assessment pursuant to article 10 (4) of Regulation (EU) 2024/1624

10 July 2026

Executive Summary

We welcome AMLA's efforts to promote greater consistency in the development and supervision of Business-Wide Risk Assessments (BWRAs) across the Union. However, several aspects of the draft Guidelines would benefit from further clarification to ensure that they support substantively risk-based, intelligence-led assessments rather than encouraging compliance-driven or prescriptive approaches.

Based on our experience with over 1,000 financial crime BWRAs across EU and non-EU jurisdictions, as well as the continuous analysis of National Risk Assessments (NRAs), Sectoral Risk Assessments (SRAs), typology reports and other intelligence sources, we propose the following key conclusions:

1. The BWRA should be recognised as an intelligence-led assessment rather than a reporting exercise. The Guidelines should clearly distinguish the purpose of the BWRA from the data collection requirements under the Draft RTS pursuant to Article 40(2) AMLD and explicitly state that compliance with the RTS does not, by itself, constitute a BWRA.
2. The Guidelines should explicitly permit digital and dynamic BWRA formats. Effective risk assessments should not be constrained to static documents where more dynamic and transparent solutions are available. Institutions should be allowed to evidence their BWRA through digital platforms, provided they remain accessible and understandable to supervisors.
3. NRAs and SRAs should be treated as important reference points, but not as primary sources for identifying inherent risks. The quality, structure and practical utility of these assessments vary significantly across Member States and sectors. They are generally most effective as a reasonableness check against an institution's own assessment rather than as the principal basis for identifying risks.
4. A stronger threat-based approach would significantly improve the usefulness of NRAs and SRAs. Rather than relying primarily on high-level risk ratings, these assessments should focus on the underlying criminal threats and risk drivers affecting a jurisdiction or sector. This would provide obliged entities with more actionable information and support more effective risk mitigation.

Acuminor
Drottninggatan 71D, 111 36 Stockholm, Sweden
acuminor.com

5. Terminology should be reviewed to ensure conceptual consistency. Greater distinction between concepts such as risk factors, risk indicators, inherent risk, exposure and residual risk would improve clarity and reduce the risk of divergent interpretation by obliged entities and supervisors.

Overall, we encourage AMLA to ensure that the final Guidelines reinforce the principle that a BWRA is an institution-specific, continuously evolving assessment of financial crime risk, informed by multiple intelligence sources, threat assessments and business-specific exposures. To be effective, the framework must prioritise substance-over-form risk identification. A framework driven primarily by prescribed inputs risks turning the assessment into a static, point-in-time exercise that fulfils tick-box regulatory reporting requirements but fails to capture actual and evolving financial crime threats and risks.

Background

Acuminor has developed the largest financial crime threat intelligence data model in the world, enabled by our proprietary analysis technology. Our comments to this public consultation are therefore informed by the continuous collection, analysis, and dissemination of hundreds of typology reports annually, including National Risk Assessments (NRAs) and Sectoral Risk Assessments (SRAs), which are incorporated into a continuously updated intelligence model containing threats and risk indicators.

Our team has experience from over 1,000 financial crime business-wide risk assessments (BWRAs) across EU and non-EU jurisdictions, ranging from small obliged entities to large global banking groups, as well as supporting regulators with sector risk assessments and law enforcement agencies with threat intelligence data.

Intelligence sources and Methodology

Paragraph 8(b): Sectoral Risk Assessments

Existing SRAs vary significantly across sectors and Member States. Some provide only high-level conclusions, such as categorising an entire sector or product as high, medium or low risk. Others provide more detailed information regarding specific threats and risk indicators. As a result, the usefulness of SRAs for inherent risk identification differs considerably.

It should be clarified that where an obliged entity's aggregated inherent risk assessment deviates from the conclusions set out in a relevant Sectoral Risk Assessment (SRA), the entity should provide a clear rationale for that divergence. For example, an institution may have limited exposure to the specific threats that drive risk within the sector and market concerned.

At the same time, SRAs should not be treated as determinative. There are cases where an SRA categorises a sector as low risk, while other credible sources indicate that the sector is significantly exposed to financial crime risks. For this reason, it would be preferable for competent authorities to explain the underlying threats and risk drivers that support a sectoral risk conclusion, rather than relying solely on high-level risk ratings. For example, identifying that a sector is heavily misused by human traffickers provides obliged entities with far more actionable information than a simple designation of high, medium or low risk.

National Risk Assessments

As with Sectoral Risk Assessments, similar observations apply to National Risk Assessments (NRAs).

Our analysis of all open intelligence sources available in Europe indicates that, on average, an EU Member State NRA contains only around 3% information that can be used by an obliged entity to identify and assess inherent risks. In some jurisdictions, this figure is 0%, with NRAs containing no information that can be readily translated into institution-specific risk assessments.

NRAs and SRAs are therefore normally too high-level to be used in isolation. In their current form, they are generally most useful as a reasonableness check against an institution's own risk assessment, rather than as a primary source for identifying and assessing inherent risks. NRAs are also often updated too seldom to provide an up-to-date, relevant view of current financial crime threats and risks.

Threat-based approach to NRAs and SRAs

More generally, it would be beneficial if NRAs and SRAs were increasingly structured around key threats (for example, human trafficking, arms smuggling etc), similar to approaches used in certain other jurisdictions such as the U.S.

There are only a few EU Member States that utilize this approach today, for example Latvia (https://www.fid.gov.lv/uploads/files/NRA%202020%20-%202022.pdf).

A clearer articulation of the principal threats affecting the Union, a Member State or a sector would support obliged entities in utilizing a holistic approach, prioritizing resources, and focusing on the most relevant risks when designing effective controls.

Preferably, the predicate offences listed in AMLD 6 would be used to define the threats that should be identified and assessed. Such an approach would also facilitate supervisory assessment of effectiveness, public-private partnerships, and support Member States and EU institutions in demonstrating outcomes during FATF mutual evaluations.

Paragraph 20

Internal intelligence sources should be considered as part of the BWRA. However, it should be clarified that Suspicious Activity Reports (SARs) and other internally generated alerts should not be the primary driver of inherent risk identification.

The reason is that SARs are typically generated as a result of existing controls, such as transaction monitoring scenarios, screening systems or investigative processes. A risk will generally only be reflected in SAR reporting if a control has already been implemented to detect it. As a result, SARs primarily provide evidence of risks that an institution has already identified and incorporated into its control framework.

From a risk management perspective, transaction monitoring and other detection controls are downstream outputs of the BWRA. The BWRA should identify and assess inherent risks, which then inform the design and implementation of controls. Consequently, over-indexing on SAR information invites confirmation bias, resulting in a myopic assessment of an obliged entity's risk environment.

We therefore recommend clarifying that SAR reporting should be considered as one relevant input among many, particularly for validating and refining risk assessments, but should not be regarded as a substitute for broader threat identification based on external intelligence, typologies, law enforcement information, sector intelligence and other relevant sources.

A similar concern has recently been raised in the context of proposed AML regulatory changes in the United States (https://www.regulations.gov/document/FINCEN-2026-0034-0001).

Aligning the EU approach with this principle would support greater consistency across global financial crime compliance frameworks and reduce the risk of divergent regulatory expectations for internationally active institutions.

Paragraph 23

Paragraph appears difficult to reconcile with the broader expectations regarding sources of information described elsewhere in the Guidelines.

The current wording states that obliged entities should begin their inherent risk identification and assessment by analysing how risks could materialise within their business and should, at a minimum, refer to the data points listed in the RTS under Article 40(2) AMLD, supplemented by additional indicators.

There is a risk that institutions will interpret this provision as establishing a complete or sufficient methodology for inherent risk identification. This implementation risk is already well known within the industry. Many obliged entities rely solely, or predominantly, on the EBA Risk Factors Guidelines when designing their BWRAs. As a result, significant resources are spent attempting to interpret how generic risk factors apply to a specific institution, even where those factors have limited or no practical relevance to the institution's actual risk profile.

The Guidelines should therefore avoid creating incentives for a similarly prescriptive approach and instead reinforce that obliged entities are expected to identify and assess risks based on their own business model, activities, exposures and dynamically evolving threat environment.

We are aware of discussions within the industry suggesting that some institutions may seek to rely primarily on the data collected under these Draft RTS as their BWRA, particularly because the data collection requirements are established through Regulatory Technical Standards (RTS), whereas the BWRA requirements are contained in Guidelines. It may also be perceived as a relatively simple and resource-efficient approach, whereby institutions focus on completing the prescribed data points and consider the assessment complete, rather than undertaking the broader analysis required for an effective BWRA.

Effective risk identification requires consideration of a much wider range of intelligence sources, internal data, law enforcement reporting and other relevant information.

The Guidelines should therefore clearly state that the data collected under the Draft Regulatory Technical Standards on the assessment of the inherent and residual risk profile of obliged entities under Article 40(2) of Directive (EU) 2024/1640 should not, by itself, be considered a BWRA, and that compliance with the RTS does not replace or fulfil the broader requirements set out in the BWRA Guidelines.

The BWRA serves a different purpose and requires a broader assessment of threats, inherent risks, controls and residual risks. Clarifying this distinction would help avoid unintended supervisory and implementation outcomes.

Terminology

"Risk Factors" vs. "Risk Indicators"

We recommend greater consistency in the use of terminology throughout the Guidelines. In particular, the term risk indicator may be more appropriate in several places where risk factor is currently used.

In practice, risk factor is commonly associated with customer risk scoring and customer risk assessment methodologies. Using the same term for broader risk identification purposes may create confusion. Distinguishing between risk factors and risk indicators would improve clarity and consistency across AML/CFT frameworks.

Paragraph 30

Paragraph 30 states that obliged entities should consider the remaining residual risks to determine their overall residual risk exposure.

We recommend reconsidering the use of the term residual risk exposure. In risk management terminology, exposure is generally associated with inherent risk, whereas residual risk reflects the level of risk remaining after controls and mitigation measures have been applied.

Using the term overall residual risk may provide greater conceptual clarity and avoid confusion between inherent and residual risk concepts.

Format and accessibility of the BWRA

The Guidelines should explicitly recognise that a Business-Wide Risk Assessment (BWRA) does not necessarily need to be produced as a static document, such as a PDF or Word report.

A digital or interactive platform may be significantly more effective than a traditional report format for institutions of all sizes. Such formats can greatly facilitate the maintenance of a risk assessment that remains dynamically updated as new information, threats, risk indicators and controls emerge or disappear. Where institutions maintain extensive intelligence repositories, source material, threat assessments and risk indicator mappings, forcing all information into a document-based format could result in reports running to thousands of pages. Such an approach may reduce rather than enhance transparency and supervisory effectiveness.

The Guidelines should therefore explicitly allow institutions to present their BWRA through digital and interactive formats, provided these are accessible to supervisors and adequately evidence the institution's assessment and conclusions.

Annex: Concrete Drafting Proposals

This Annex sets out concrete drafting proposals for specific paragraphs of the draft Guidelines, reflecting the comments and conclusions set out above. For each item, the paragraph reference of the draft Guidelines is given, followed by the proposed new or amended text.

Paragraph 2 (Definitions) – insert new sub-paragraph (d)

Terminology: distinguishes the customer-level concept of 'risk factor' (EBA/GL/2021/02) from the business-wide concept used throughout the BWRA Guidelines.

'Risk indicators' means variables, patterns, threats or other evidence, either on their own or in combination, that inform the identification and assessment of the obliged entity's business-wide inherent risks of ML/TF and non-implementation and evasion of TFS.

New paragraph – insert after paragraph 5 (Key principles)

Comment related to the BWRA should be recognised as an intelligence-led assessment, distinct from the RTS Article 40(2) data collection exercise.

The BWRA is an intelligence-led, institution-specific assessment of the obliged entity's ML/TF and non-implementation and evasion of TFS risk exposure. Compliance with the data collection requirements of the Regulatory Technical Standards on the assessment of the inherent and residual risk profile of obliged entities under Article 40(2) of the AMLD does not, by itself, constitute a BWRA, and does not replace or fulfil the requirements set out in these guidelines, which serve a distinct purpose and require a broader assessment of threats, inherent risks, controls and residual risks.

Paragraph 5(a) – replace

Section 'Format and accessibility of the BWRA': the Guidelines should explicitly permit digital and dynamic BWRA formats.

Put in place policies, procedures and controls to ensure that the BWRA is documented, kept up-to-date and reviewed regularly so that it remains accurate and aligned with the OE's risk exposure. The BWRA does not need to be evidenced through a static document (such as a PDF or Word report); OEs may evidence their BWRA through digital, dynamic or interactive formats, provided these remain accessible, retrievable and understandable to supervisors upon request in accordance with paragraph 5(e);

Paragraph 15 – replace

Terminology: 'risk indicator' rather than 'risk factor' for business-wide risk identification.

When assessing ML/TF/non-implementation and evasion of TFS risks, OEs should apply a risk-based weighting of relevant risk indicators, assigning more weight to those indicators that have greater impact on their overall risk exposure. OEs should document the rationale behind any weighting decisions in their methodology, ensuring it is clear how each indicator's significance was determined. For this purpose, OEs should make informed, evidence-based judgements about the relevance of

each risk indicator in the context of their business model, and the corresponding predicate offences (threats) to which relevant risk indicators are connected.

Paragraph 16 – replace

Terminology: 'risk indicator' rather than 'risk factor'.

OEs should design a BWRA methodology that produces clear, accurate, and reliable outcomes. Such a methodology should include risk rating levels appropriate for the OE's size, nature, and ML/TF/non-implementation and evasion of TFS risk exposure, ensuring no single risk indicator disproportionately drives the overall outcome. Where an OE's risk rating levels diverge from those expected in the Annexes II and III of the AMLR or in EU or Member State risk assessments conducted under Articles 7 and 8 of the AMLD, the rationale for these ratings should be clear.

Paragraphs 8a and 8b

Comments related to current SRA/NRA shortcomings and usability when used by OEs to perform BWRA.

OEs should treat National Risk Assessments (NRAs) and Sectoral Risk Assessments (SRAs) referred to in Article 10(1) of the AMLR as an important reference point and as a reasonableness check against their own inherent risk identification, rather than as the principal or sole source for identifying inherent risks, given that the level of detail and underlying threat information contained in NRAs and SRAs varies significantly across Member States and sectors.

Where an OE's aggregated inherent risk assessment diverges from the conclusions of a relevant NRA or SRA, the OE should document a clear rationale for that divergence, for example where the OE has limited exposure to the specific threats driving the risk conclusion concerned.

Paragraph 20 – replace

Comments on Paragraph 20: SARs and internal alerts should not be the primary driver of inherent risk identification.

When conducting their BWRA, OEs should also make use of: their own knowledge and professional expertise derived from Suspicious Transaction Reports or Suspicious Activity Reports submitted to the FIU, as well as requests for information or feedback received from FIUs, law enforcement or judicial authorities; and internal insights, including findings from compliance and internal audit reviews and lessons learned from supervisory actions. Information under this paragraph should be considered as one relevant input among others, used in particular to validate and refine the OE's risk assessment, and should not be treated as the primary basis for identifying inherent risks, given that Suspicious Transaction Reports, Suspicious Activity Reports and other internal information generally reflect risks already captured by an OE's existing detection controls rather than risks not yet identified.

Paragraph 23 – replace

Comments on Paragraph 23: risk of the RTS Article 40(2) data points being read as a sufficient methodology; terminology ('risk indicator').

OEs should begin their inherent risk identification and assessment by analysing how ML/TF/non-implementation and evasion of TFS risks could materialise within their business, including any emerging risks, by taking a holistic view of all relevant risk indicators related to customer, product/service/transaction, delivery channels and geographical exposure. This analysis must draw on the broad range of external intelligence sources, internal data and other relevant information referred to in Section 2.2, reflecting the OE's own business model, activities and dynamically evolving threat environment. OEs may refer to the data points listed in the RTS on Article 40(2) of the AMLD as one input among others, as long as all other relevant sources in this Guideline are also used. Compliance with RTS Arcticle 40(2) does not, on its own, constitute a sufficient or complete methodology for identifying and assessing inherent risks under these guidelines.

Paragraph 24 – replace

Terminology: 'risk indicator' rather than 'risk factor'.

When classifying inherent risks that are relevant to their business, OEs should assess their exposure to the identified risk indicators using the most suitable method. The assessment should enable a meaningful, proportionate understanding of inherent risks, reflecting the OE's business model and operational realities.

Paragraph 30 – replace

Comments on Paragraph 30: 'exposure' is an inherent-risk concept and should not be paired with 'residual risk'.

Apart from assessing the residual risks associated with each risk indicator, OEs should determine their overall residual risk.