14 July 2026

EBF feedback on AMLA draft guidelines on Business-wide risk assessment under Article 10 (4) of Regulation (EU) 2024/1624

Question 1: Do you agree that the proposals set out in these draft GLs can be applied across all obliged entities and allow for an effective application of a risk-based and proportionate approach towards compliance with AML/CFT requirements?

If not, please:

(i) specify the provision concerned with clear reference to the paragraph; and

(ii) provide concrete drafting proposals and explain why the specific measures you propose would be more appropriate.

Comment 1 – Paragraphs 3 and 6:

We acknowledge and support the overarching principle laid down in paragraphs 3 and 6 of the Guidelines confirming that the BWRA should be proportionate to the nature and size of the business and should not be carried out as a mere formalistic exercise. In this context, we note that certain minimum requirements proposed for the BWRA may prove operationally challenging in practice and could be subject to broad interpretation.

Against this background, and with regard to the applicability of the Guidelines to all obliged entities, we believe that our proposed amendments below could help provide more clarity and further strengthen the risk-based approach as set out in the aforementioned paragraphs.

Comment 2 – Paragraph 11:

Par. 11 provides that parent undertakings should ensure that all branches and subsidiaries conduct their own BWRAs. We believe this should instead reflect a risk-based approach that considers the legal nature and functions of branches. The level for the BWRA to be performed should be adapted to the group's internal organization. While a consistent group-wide approach is important, the GLs should not imply that all entities must apply an identical methodology /template. In line with Art. 16(1) AMLR and the draft RTS under Arts. 16(4) and 17(3) AMLR, BWRAs should contribute to a coherent group-wide risk assessment through harmonised minimum standards, while allowing third country subsidiaries sufficient flexibility to adapt their assessments to local legal and supervisory requirements. Such flexibility is necessary to ensure compliance with local legal obligations while preserving consistency across the group and avoiding unnecessary duplication. It should be noted that Article 16 AMLR explicitly allows OEs being the parent undertaking to consider the specificities and the risks of their group entities to which they are exposed when it comes to implementing group wide requirements.

European Banking Federation aisbl
Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

Unlike subsidiaries, branches are extensions of the parent undertaking rather than separate legal entities. Depending on the group's organisation, AML/CFT and TFS risks relating to branches may already be captured within the parent's BWRA. In addition, some branches or subsidiaries perform only operational or back-office functions and do not establish customer relationships, making a separate BWRA unlikely to provide additional value. Requiring separate assessments in such cases would create additional operational burden without enhancing the institution's understanding or management of risk.

AMLA should clarify that the group-wide risk assessment under Art. 16(1) AMLR is required only at the level of the EU parent undertaking (or designated EU sub-consolidating entity), and not at each intermediate holding company. We therefore propose inserting the following par. after par. 11: "*Group parent undertakings should assess, on a risk-based basis, whether branches should conduct their own BWRAs or contribute directly to the BWRA of the parent entity. This assessment should take into account the size, complexity and activities of the branch, including whether it provides services to customers or performs supporting or back-office functions*."

AMLA should also explain whether "consolidation" means aggregating entity-level BWRAs or conducting an integrated analysis of group-wide risks, and whether residual risk should be assessed by risk category or only at overall group level.

Comment 3 – Paragraph 10

AMLA should clarify that recommendations in these guidelines are not intended to govern the way in which the BWRA is practically formalized, which may vary from case to case for legitimate reasons relating to the activities carried out and existing well-established local practices endorsed by supervisors in various Member States. Otherwise, paragraph 10 would not be in line with AMLA's overarching principle to provide obliged entities methodological flexibility.

For instance, we request that AMLA clarify that paragraph 10's requirement to aggregate assessments for distinct business areas into a single entity-level BWRA does not mandate the production of a single physical document, provided that the documentation maintained provides a sufficiently clear and comprehensive overview of the entity's overall ML/TF risk exposure.

Comment 4 – Paragraphs 6

The organisational structures of financial institutions often feature multiple financial holding companies – most commonly for asset protection purposes. These holding companies have no clients or actual business activities.

We acknowledge that, where a financial holding company acts as a group parent undertaking, it should be responsible for carrying out a group-wide risk assessment pursuant to Article 16 of the AMLR. However, we question the need for such an entity or another intermediary financial holding company to perform their own BWRA (at entity level). In such cases, the exercise would become formalistic, contrary to para. 6.

We further note that such entities would not fall under the exemptions mentioned in para. 8. While these exemptions refer to the RTS under Article 40(2) of the AMLD6, the conditions laid down in this article do not cover financial holding companies which do not engage in any of the exempted activities (as their activity is highly limited). We therefore propose adding a paragraph clarifying that obliged entities, which are part of a group, but do not serve clients, should not be required to conduct their own BWRA at entity level:

"*Obliged entities that do not serve clients and/or do not conduct any transactions do not need to perform a BWRA at entity level. However, obliged entities acting as parent undertakings of a group remain responsible for the performance of a group-wide risk assessment*".

Additionally, the "structure" as defined in the draft RTS related to Group-wide requirement (Art 16(4) and 17(5) of the AMLR) should be out of scope of the requirement to perform BWRA and therefore shall not be considered by parent undertakings when they perform a Group-wide risk assessment.

Comment 5 – Paragraph 8 (a):

Para. 8(a) states that non-complex obliged entities may apply a less elaborate BWRA and opt for a more qualitative and descriptive assessment. It further defines as 'non-complex' those entities that cumulatively meet the criteria in terms of size and activity for reduced frequency of the supervisory risk assessment pursuant to the RTS on Article 40(2) of the AMLD6.

We note that the Guidelines appear to adopt a stricter approach than the RTS in question. Whereas the Guidelines require that the criteria are cumulatively met, Article 5(3) of the final draft RTS introduces the criteria alternatively ("where the credit institution or financial institution meets *any* of the following criteria:"). We hence suggest aligning the wording of the Guidelines with that of the RTS.

Moreover, we highlight that certain obliged entities which do not serve clients, do not conduct transactions, and have very limited business activities (i.e. financial holding companies) should be out of scope. We therefore reiterate our proposal stipulated in Comment 4.

Comment 6 – Paragraph 5(a)

Paragraph 5(a) requires the BWRA to be 'kept up-to-date' but does not define what constitutes a material change requiring an ad hoc update. We request that AMLA amend paragraph 5(a) to confirm that a review resulting in no substantive amendment is a valid outcome, provided it is documented and approved.

We also request that AMLA confirm how the review expectations in paragraph 5(a) will interact with the forthcoming Guidelines on Article 9(4) AMLR, to avoid divergent or duplicative review obligations.

Comment 7 – Paragraph 15:

When assessing ML/TF as well as non-implementation and evasion of targeted financial sanctions (TFS) risks, obliged entities are expected to apply a risk-based weighting of relevant risk factors, assigning greater weight to those that have the most significant impact on their overall risk exposure. They are also required to document, within their methodology, the rationale for these weighting decisions.

The requirement to document the methodology, weighting and scoring approach should not be interpreted as requiring an overly granular justification of each individual parameter where this would not be proportionate. Rather, obliged entities should retain sufficient flexibility to apply a methodology that is tailored to their specific risk profile, while ensuring appropriate transparency and governance.

We also request clarification on the concept of 'evidence-based judgements' in paragraph 15. In practice, any judgement as part of a BWRA methodology should follow a pre-defined process and governance, which is part of the methodology itself, and should be understood against the background of quantitative and qualitative data requiring expert knowledge. Insofar, usage of subject-matter experience is quite common. Requiring explicit evidence in the sense of purely quantitative data without allowing subject-matter expert judgement is not feasible and does not provide meaningful outcomes. We therefore suggest replacing 'evidence-based' with 'reasoned and appropriately documented judgements (including subject matter expert judgements), supported by defined methodology and governance'.

Comment 8 – Paragraph 23:

According to par. 23:" 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 factors related to customer, product/service/transaction, delivery channels and geographical exposure. For this purpose, OEs should at least refer to the data points listed in the RTS on Article 40(2) of the AMLD, supplemented by any additional relevant quantitative and qualitative indicators such as strategic plan modifications, mergers or regulatory changes. We note that par. 23 uses the formulation "should at least refer to" confirming that these categories constitute a minimum set. This requirement does not appear proportionate, as not all data points set out in the RTS are relevant to every type of OE. The RTS should therefore not be interpreted as establishing a mandatory minimum dataset applicable to all entities, but rather as providing a catalogue of data points from which OEs should select those that are relevant to the purposes of their Business-Wide Risk Assessment. It should also note that obliged entities may supplement these categories with additional risk factors relevant to their specific risk profile. The Guidelines should provide flexibility for obliged entities in how the RTS Art. 40 (2) AMLD6 data points are applied and to align the data points with each entity's specific BWRA methodology.

In order to avoid any ambiguity, we suggest amending paragraph 23, as follows:

"For this purpose, OEs may refer where relevant and appropriate to the data points listed in the RTS on Article 40(2) of the AMLD, supplemented by any additional relevant quantitative and qualitative indicators such as strategic plan modifications, mergers or regulatory changes with a focus on their aggregated impact at the business wide level".

Question 2: Do you agree with the proposed minimum requirements for the content of the BWRA set out in these draft GLs?

If you do not agree, please specify:

(i) the provision(s) concerned, with clear reference to the paragraph; and

(ii) the rationale for your position.

Please provide concrete drafting proposals to resolving the issue and explain why the measure you propose would be more appropriate.

Comment 1 – Paragraph 32:

We agree that the BWRA should lead to timely remediation of identified weaknesses. However, paragraph 32 would benefit from clarifying that the BWRA should identify remediation priorities, while the detailed implementation of mitigating measures may be reflected in the obliged entity's policies, procedures and controls. This would help avoid unnecessary duplication between the BWRA and the broader internal control framework.

Proposed amendment to para. 32:

"Upon completion of the BWRA, OEs should determine the priority areas for action and ensure timely implementation of the necessary remediation measures. The BWRA should identify the resulting remediation priorities, while the detailed implementation of those measures may be reflected in the OE's policies, procedures, systems and controls."

Comment 2 – Paragraph 21:

Paragraphs 21/22 require obliged entities to prepare a business and operational overview as the starting point for the BWRA.

Clarification is needed as to whether the BWRA is intended to replace or consolidate existing risk cartography and risk classification exercises, or to coexist as a distinct but overlapping framework. This is necessary to understand the expected balance between quantitative, qualitative or hybrid approaches, and to avoid duplication of effort. We note that the AML function of each obliged entity and foreign branch already prepares an annual 'Report on the risks of ML, TF and FS' covering the respective year and submitting it to the management/supervisory board, as required by existing EBA guidelines (EBA/GL/2022/05 on AML/CFT compliance officers and EBA/GL/2024/14 on restrictive measures). We request clarification as to whether such an activity report is considered

sufficient to satisfy the 'business and operational overview' requirement of Minimum Requirement 1.

We also suggest adding the words 'to the extent deemed relevant or material to the OE' after 'outsourcing arrangements and any use of new or emerging technologies' in paragraph 21. This would help avoid an interpretation whereby obliged entities are expected to document all arrangements or technologies with the same level of detail, regardless of their materiality from an AML/CFT perspective.

Comment 3 - Paragraph 5 (c)

Paragraph 5(c) provides that the BWRA is ”drawn up by the Compliance Officer, approved by the management body in its management function in accordance with Article 10(2) of the AMLR and, where such body exists, communicated to the management body in its supervisory function.”

The wording “drawn up by the Compliance Officer” is currently ambiguous as to whether it requires sole personal authorship within the second line of defence, or whether it permits the Compliance Officer to coordinate a cross-functional drafting process with substantive input from the first line of defence (commercial functions), consistent with the three lines of defence governance model.

The guidelines should clarify that 'drawn up by the Compliance Officer' denotes accountability for the methodology, process and final output, and does not preclude a collaborative approach under the Compliance Officer's direction, while the underlying risk assessment is informed by and populated with inputs from the first line of defence. This interpretation would be consistent with proportionate, risk-based governance principles.

Comment 4 – Paragraph 15

The requirement to document the methodology, weighting and scoring approach should not be interpreted as requiring an overly granular justification of each individual parameter where this would not be proportionate.

Rather, obliged entities should retain sufficient flexibility to apply a methodology that is tailored to their specific risk profile, while ensuring appropriate transparency and governance.

We therefore suggest that paragraph 15 clarify that obliged entities should document the methodology applied, the categories of sources considered, and their relevance to the BWRA.

Comment 5 – Paragraph 16

Paragraph 16 requires that obliged entities explain any divergence between their BWRA risk ratings and the expectations set out in Annexes II and III of the AMLR. However, Annexes II and III only provide for potentially lower or higher risk factors and are designed for use at individual risk assessment level (customer or transaction), not for portfolio-level classification. The application of individual-level risk factors at BWRA level is not straightforward and risks distorting the entity-level assessment. We propose that AMLA

amend paragraph 16 to clarify that: (a) Annexes II and III serve as reference points for individual risk assessments; (b) for BWRA purposes, obliged entities should consider the aggregate distribution and concentration of the relevant risk factors across their portfolio; and (c) 'divergence' refers to systematic and unexplained inconsistencies between the BWRA's overall risk conclusions and the risk signals generally associated with the entity's portfolio composition, not to factor-by-factor mechanical alignment.

We suggest amending paragraph 16 as follows: *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 factor disproportionately drives the overall outcome.* ***OEs should ensure that their BWRA also reflects the steps taken to assess the ML/TF risk associated with individual business relationships or occasional transactions and their ML/TF risk appetite.***

Question 3: Do you agree with the proposals for additional sources of information to be taken into account when carrying out the BWRA set out in these draft GLs?

If you do not agree, please specify:

(i) the sources you disagree with; and

(ii) the rationale for your position;

(ii) the sources that should be included.

The additional sources of information—also reflected in the existing EBA Guidelines (EBA/GL/2021/02)—should be understood as supplementary and not inherently mandatory.

We note that the list of additional sources of information laid down in para. 19 is extremely extensive. Reading the paragraph in conjunction with para. 18, it is our understanding that the type and number of sources to be considered depends on the obliged entity's nature and business complexity.

However, the wording of para. 19, namely "the following non-exhaustive list of additional sources of information is to be taken into account", seems to imply that all listed sources need to be considered. Such an interpretation would not appear fully consistent with the principle of proportionality, particularly given that the text itself refers to the selection of sources according to the nature and complexity of the institution. It may therefore be helpful to clarify that the list of additional information sources is illustrative rather than exhaustive, and that institutions should select those sources that are relevant to their specific risk profile, while appropriately documenting the rationale for their selection. Absent such clarification, an obligation to consider the full list could lead to significant additional costs and operational effort, as the current wording may create overly broad expectations.

We would therefore propose amending para. 19 to state the following:

"In this regard, obliged entities may choose among the following non-exhaustive list of additional sources of information when preparing their BWRA:".

We also request that the sources be aligned with the list of sources listed in Level 1 and removal of the below.

- Information from public authorities and official authorities such as fraud observatories, central banks, statistical organisations and academia.
- Information from sanctions and watchlists maintained by competent authorities to identify persons, entities, jurisdictions or patterns relevant to ML/TF and TFS evasion risks.
- Industry-level and professional sources of information shared by relevant industry bodies, professional associations or SRBs, including public-private partnerships and inter-agency cooperation forums.
- Information from civil society, such as corruption indices and country reports
- Information from credible and reliable commercial organisations, such as risk and intelligence reports.

Furthermore, the Guidelines do not provide a definition of what constitutes "reliable" and "credible" sources within the meaning of Paragraph 19. It is unclear whether AMLA has specific expectations regarding how obliged entities should document their consideration of source information, including instances where certain sources are assessed as not relevant. Clarification is also requested on how obliged entities are expected to ensure the ongoing maintenance and governance of the list of sources, in particular whether a formal periodic review (e.g. annual review) is required.

To enhance clarity, we suggest the following further amendments:

- (i) amending paragraph 18 (second sentence) by inserting "on a risk-based approach", resulting in: "In all cases, OEs should determine on a risk-based approach the type and number of sources of information considered […]" and(ii) similarly adjusting paragraph 20 by replacing "should also make use of" with "should also consider when deemed relevant", in line with the current EBA Guidelines.
- Finally, with regard to paragraph 17, while we acknowledge the need for transparency concerning the sources of information used, this should not result in an overly administrative burden. We therefore recommend either removing the wording "and in the manner in which such sources were used" or clarifying it to allow flexibility, rather than requiring detailed, factor-by-factor mapping across all sources.

Question 4: Do you foresee any operational challenges in implementing these GLs?

If so, please specify:

(i) the provision(s) concerned with clear reference to the paragraph; and

(ii) the rationale for your position.

Comment 1 – Paragraph 11:

With regard to para. 11, operational challenges would arise in relation to the establishment of a common methodology which caters for all different types of entities comprising larger, cross-border groups. In practical terms, a large group may be composed of financial holding companies, credit institutions, and other financial institutions (e.g. insurance companies, central securities depositories, payment service providers, etc.). This renders the design of a detailed methodology particularly difficult.

In addition, practical challenges may arise where a common methodology is interpreted as requiring a uniform template or format across all entities within the group. For subsidiaries operating in different jurisdictions, such an approach may not align with local supervisory expectations or legal requirements. While consistency of core elements is desirable, a degree of flexibility in the structure and presentation of the BWRA is necessary and appropriate to reflect local context and varying levels of complexity. Consequently, a common methodology in the context of such diverse groups should serve as a high-level framework, rather than imposing uniform granular requirements across the group. We recognise that (in line with Art. 16 (1) AMLR) para. 11 specifies that the methodology should reflect the specific risks and characteristics of entities' individual operations. Nonetheless, we would further emphasize that it should further cater for cases where the types of entities differ, including the inherent risk factors applicable to them pursuant to RTS on Article 40(2) of the AMLD.

Therefore, to provide further clarification, we propose inserting the following paragraph in Section 2.2 (Methodology and Sources of Information):

"Obliged entities acting as the parent undertaking of a group should ensure that the common methodology referred to in para. 11 covers at least the Minimum Requirements listed in Section 2.3. When deciding on the level of detail of the common methodology, OEs acting as parent undertakings should consider the type of entities comprising the group and the diversity of the business activities they perform."

We would also draw AMLA's attention to the fact that requiring the parent entity to coordinate and harmonize a common methodology for the whole group may directly challenge decentralized organizations based on subsidiarity (e.g. cooperative banking groups) where such matters are collectively agreed upon by local stakeholders rather than decided top-down.

Therefore, the guidelines should clarify that the requirement for parent undertakings to ensure that a coordinated approach/common methodology may be achieved through

various means depending on the group structure. This may take forms other than direct reporting lines between the group and entity level, for instance, through committees bringing together all stakeholders involved in the drafting of the BWRA.

Comment 2 - Sources of information – paragraph 17

We would suggest clarifying that the obliged entities should document the categories of sources relied upon and their relevance to the BWRA, rather than being required to evidence an exhaustive review of all available sources. The use of sources should therefore remain risk-based, proportionate, and operationally manageable. An overly broad interpretation of the obligation to document all sources consulted and how they have been used, could undermine the principle of proportionality and create a disproportionate operational burden, particularly for less complex or lower-risk entities.

Comment 3 – Paragraph 23:

Paragraph 23 states that, when implementing Minimum Requirement 2, obliged entities should 'at least refer to the data points listed in the RTS on Article 40(2) of the AMLD'. Not all data points in the RTS are applicable to all types of obliged entities. The RTS should not be interpreted as establishing a mandatory minimum set of data points, but rather as a catalogue from which obliged entities select those data points relevant for the purposes of their Business-Wide Risk Assessment. Therefore, we suggest specifying in the wording of the paragraph that OEs should may consider the data points applicable to them, as not all data points in the RTS apply to all types of entities.

We propose that AMLA confirm: (a) that obliged entities are required to consider and document their assessment of each applicable RTS data point as a reference input, without being required to restructure their BWRA to mirror the RTS categorisation. AMLA should therefore clarify that the data points listed in the RTS on Article 40(2) of the AMLD may be adapted to the obliged entity's existing data structures (for example, by using client relationships rather than customers as the counting unit); and (b) that transitional guidance will be issued once the RTS is finalised, clarifying the interaction between the final RTS and the BWRA methodology requirements.

We also request that AMLA clarify whether a proportionate 'de-scoping' approach is acceptable, whereby obliged entities that assess certain risk factors as not material to their specific business model may document the rationale for non-assessment rather than performing a full assessment, and if so, what standard of documentation is required.

Furthermore, we note that the timelines for AMLA reporting and the annual BWRA may not be aligned, meaning that RTS data points will not always be up-to-date at the time the BWRA is performed. This is particularly relevant for the initial BWRA in 2027.

There should also be flexibility in how these data points are applied, as this may vary across organisations and sectors, and should be aligned with each entity's specific BWRA methodology. To avoid any ambiguity, we propose amending the wording as follows:

"For this purpose, OEs may refer where relevant and appropriate to the data points listed in the RTS on Article 40(2) of the AMLD, supplemented by any additional relevant

quantitative and qualitative indicators such as strategic plan modifications, mergers, or regulatory changes, with a focus on their aggregated impact at the business-wide level."

Comment 4 - paragraph 10

Paragraph 10 states that OEs should assess whether separate business areas require separate assessments. We note that this widens the scope of who should consider conducting a BWRA. Clarification is requested regarding how the regulator intends the concept of a "business area" to be interpreted and operationalised for the purposes of the BWRA.

Comment 5 – Paragraph 24

We recommend that the Guidelines explicitly confirm the freedom of an OE that is a parent undertaking to determine the most appropriate methodology for assessing its risks at group level and to apply this same methodology to the individual risk assessments of all its subsidiaries and branches in the EU/EEA, which are required to submit such assessments as OEs in their own right to their respective NCAs.

Accordingly, we propose adding wording along the following lines:

"For OEs that are parent undertakings, the chosen method shall also be used for the individual risk assessments submitted by their subsidiaries and branches in the EU/EEA to the relevant NCAs."

Comment 6 - Paragraph 26

While the term "evidence-based view" in paragraph 26 is conceptually valid, in practice—particularly for large and complex organisations—it could be interpreted as requiring evidence for a vast number of individual control instances to support assessments of effectiveness, which would not be practical.

To ensure transparency and objectivity in assessing control effectiveness, it is more appropriate to focus on the existence of a robust framework, clear processes and sound governance. We therefore propose revising paragraph 26 to state: "OEs should be able to demonstrate a clear process and governance to conclude on whether current policies, procedures and controls are effectively mitigating inherent risks and where gaps or weaknesses remain."

This formulation clarifies that an "evidence-based view" should be reflected in demonstrable processes and governance structures that substantiate effective risk mitigation, rather than merely asserting such a view.

Comment 7– Paragraph 28:

We support the assessment of control quality under paragraphs 25 to 28. However, the draft should clarify more explicitly that the depth and evidentiary basis of such assessments should remain proportionate to the nature, scale and complexity of the obliged entity.

Without such clarification, the draft may be interpreted as requiring overly formalised control-testing frameworks also for smaller or less complex entities.

Proposed addition after para. 28:

"The depth and evidentiary basis of the assessment referred to in paragraphs 25 to 28 should be proportionate to the nature, scale and complexity of the obliged entity and to the risks to which it is exposed."

Comment 8 - paragraph 5.d

Paragraph 5(d) states that OEs should: "Take steps, including ongoing training, to ensure that their employees or persons in comparable positions whose function so requires, including agents and distributors, are aware of and understand the BWRA and how it affects their daily work in line with Article 12 of the AMLR"

We request clarification on the target audience for this training obligation, in particular whether its primary purpose is to cover employees directly involved in conducting the BWRA. If this is the intended scope, the obligation should be limited accordingly and the wording could be clarified as follows:

"to take steps, including ongoing training, to ensure that employees or persons in comparable positions whose function involves conducting the BWRA, including agents and distributors, are aware of and understand the BWRA"

More broadly, it should be clarified how the training obligation should be implemented and that it should apply on a role-based and need-to-know basis. Relevant staff should be made aware of the practical implications of the BWRA for their day-to-day activities, including applicable risk factors, vigilance measures and mitigation actions. However, they should not be expected to master the full technical methodology, scoring model or weighting approach unless this is relevant to their role. In particular, training on the assessment of control quality should be tailored to the functions concerned, as such level of detail would not be relevant for staff who do not perform control, testing or inspection-related tasks.

Comment 9 - Paragraph 29

Paragraph 29 states that OEs should determine the residual risk they remain exposed to, taking into account the inherent risk level and the overall effectiveness of the control environment. Paragraph 30 then requires OEs to consider "remaining residual risks" to determine their overall residual risk exposure.

The current wording of paragraphs 29 and 30 creates ambiguity in the interpretation of "residual risks", particularly through the references to "residual risks associated with each inherent risk" and the subsequent consideration of "remaining residual risks".

In our view, this wording may be understood as suggesting a largely linear or one-to-one relationship between inherent risks, controls and residual risks. However, in practice - especially in large and complex organisations—risk mitigation does not operate on a one-

to-one basis. Instead, inherent risks are typically addressed through multiple, overlapping controls operating at different stages of the control framework (e.g. preventive, detective and downstream), resulting in a many-to-many relationship.

Accordingly, residual risk should be interpreted as the outcome of an aggregated assessment in which:

- inherent risks are assessed across multiple risk drivers, and
- the effectiveness of the control environment is considered holistically, taking into account the combined and interdependent impact of multiple controls and mitigating measures.

Against this background, the notion of "remaining residual risks" should be clarified as referring to the overall residual risk exposure at the level of the OE, rather than implying a separate or additional analytical layer beyond the assessment of residual risk per inherent risk.

Without such clarification, there is a risk that the Guidelines may be interpreted in a way that leads to overly granular and operationally burdensome methodologies (e.g. strict one-to-one mappings between risks and controls), which would not necessarily improve the effectiveness of the BWRA and could detract from its core function as a risk management tool.

Question 5: Within the boundaries of the mandate as defined in Article 10(4) AMLR, do you identify any need to introduce additional provisions?

If so, provide concrete drafting proposals.

We recommend that the Guidelines explicitly confirm the freedom of an OE that is a parent undertaking to determine the most appropriate methodology for assessing its risks at group level and to apply this same methodology to the individual risk assessments of all its subsidiaries and branches in the EU/EEA, which are required to submit such assessments as OEs in their own right to their respective NCAs.
Accordingly, we propose adding wording along the following lines:

"For OEs that are parent undertakings, the chosen method shall also be used for the individual risk assessments submitted by their subsidiaries and branches in the EU/EEA to the relevant NCAs."

We also suggest the following additional specifications and clarifications that would materially support practical implementation:

- **Par.16:** The reference to ensuring that no single risk factor "disproportionately drives the overall outcome" would benefit from more specific guidance.
- **Section 3.3:** Section 3.3 of the consultation paper states that individual risk assessments (IRA) conducted under Article 20(2) AMLR and the BWRA should mutually inform each other but provides no guidance on how this is to be implemented in practice. We suggest supplementing Section 3.3 with a dedicated sub-paragraph in the Guidelines specifying the nature of expected IRA inputs, update triggers, and proportionate documentation standards.

- In **Section 3.2** of the consultation paper on Proportionality and simplification, it is stated that "the level of detail and elaboration of the BWRA should be aligned with the complexity of the OE's structure, with the aim of reducing the burden for less complex OEs". Clarification is requested on how "complexity of the OE's structure" should be interpreted in this context. In particular, it should be specified whether this refers to:

    i) the overall complexity of the obliged entity considered on an aggregated basis, or
    ii) the complexity of each individual subordinate institution.

- **Par. 25** requires obliged entities to assess how effectively their AML/CFT policies, procedures and controls mitigate identified risks by 'clearly linking them together and explaining how the control mitigates the risk in practice'. In practice, however, many procedures and controls are difficult, if not impossible, to link to one specific inherent risk only (e.g. governance structures, internal policies or AML training programmes). Their mitigating effect arises from the control framework as a whole. The relationship between risks and controls is typically many-to-many/non-bijective, rather than one-to-one. A single control may mitigate multiple risks and, conversely, several controls may jointly address a single risk. As a result, establishing a strictly granular mapping between individual risks and controls would be difficult to implement in a consistent, scalable and proportionate manner across institutions. In this regard, further guidance would be welcome on the expected level of granularity and formalisation in mapping risks to controls, in order to ensure that the requirement supports traceability and transparency without leading to overly complex or artificial mapping frameworks. We therefore suggest clarifying that obliged entities may demonstrate risk mitigation either by linking specific controls to identified inherent risks, or by explaining how the overall framework of controls, taken as a whole, mitigates an individual risk and supports the reduction from inherent risk to residual risk. Proposed addition to paragraph 25: *"…or by explaining how the framework of procedures and controls as a whole has a mitigating influence on an individual risk."*