EBA RESPONSE TO THE EUROPEAN COMMISSION'S CALL FOR ADVICE ON SIX AMLA MANDATES

EBA/REP/2025/35 OCTOBER 2025

Table of Contents

Abbreviations

AMLD6	The sixth Anti-Money Laundering Directive
AMLR	Anti-Money Laundering Regulation
AMLAR	Regulation establishing the Anti-Money Laundering Authority
AML	Anti-money laundering
AMLSC	Standing Committee on Anti-Money Laundering and Countering Terrorist Financing
CA	Competent authority
CASP	Crypto assets service provider
CDD	Customer due diligence
CIU	Collective investment undertakings
CFT	Countering the financing of terrorism
EDD	Enhanced due diligence
EMI	E-money institution
EMT	Electronic money token
EuReCA	European Reporting system for material CFT/AML weaknesses
FIU	Financial intelligence unit
FTR	Funds Transfer Regulation
LEA	Law enforcement authority
LIU	Life insurance undertaking
LII	Life insurance intermediaries
MiCA	Markets in Crypto Assets Regulation
ML	Money laundering
NRA	National risk assessment
PEP	Politically exposed person
PSD2	Payment Service Directive 2
PSP	Payment service provider
RTS	Regulatory technical standards
SEPA	Single euro payments area
STR	Suspicious transaction report
TF	Terrorist financing
UBO	Ultimate beneficial owner
vIBAN	Virtual international bank account number

Executive Summary

On 12 March 2024[1], the EBA received a Call for Advice (CfA) from the European Commission on certain draft regulatory technical standards (RTS) under the new EU AML/CFT framework. The EBA's response to the CfA will inform the work of the new AML/CFT Authority (AMLA).

The CfA covers the following mandates:

- The mandate, under Article 40(2) of Directive (EU) 2024/1640 (AMLD6), to develop draft regulatory technical standards on the assessment and classification of the inherent and residual risk profile of obliged entities and the frequency at which such profile must be reviewed;
- The mandate, under Article 12(7) of Regulation (EU) 2024/1620 (AMLAR), to develop draft regulatory technical standards on the risk assessment for the purpose of selection for direct supervision;
- The mandate, under Article 28(1) of Regulation (EU) 2024/1624 (AMLR), to develop draft regulatory technical standards on customer due diligence (CDD);
- The mandate, under Article 53(10) AMLD6, to develop draft regulatory technical standards on pecuniary sanctions, administrative measures and periodic penalty payments.

In addition, the Commission asked the EBA to set out options AMLA should consider when taking up work on two additional mandates:

- guidelines on base amounts for pecuniary fines under Article 53(11) AMLD6.
- draft regulatory technical standards on group-wide policies and procedures under Article 16(4) AMLR.

This Report includes the EBA's proposals for the draft regulatory technical standards ("RTSs") mentioned above, as well as preparatory work on the two additional mandates. They provide a solid foundation for a resilient EU AML/CFT system in line with AMLA's statutory objectives. When putting together its proposals, the EBA was guided by the principles of a proportionate, risk-based approach that can be applied effectively by financial institutions and their AML/CFT supervisors and is conducive to limiting the cost of compliance where possible.

It will fall to AMLA, in consultation with the Commission, to take these proposals forward.

[1] https://www.eba.europa.eu/sites/default/files/2024-03/2d15a537-adaa-49ce-8b2a-54467772dfb6/CfA%20RTSs_GL%20EBA_fin_rev.pdf.

1. Background and rationale

1.1 Background

1. On 12 March 2024, the EBA received a Call for Advice (CfA) from the European Commission (EC) on certain draft regulatory technical standards (RTS) under the new EU AML/CFT framework.

2. The CfA includes a mandate under Article 12(7) of Regulation (EU) 2024/1620 (AMLAR) on the risk assessment for the purpose of selection for direct supervision and a mandate under Article 40(2) AMLD6 on the methodology for assessing the inherent and residual risk profile of obliged entities.

3. The CfA also includes a mandate under Article 28(1) of Regulation (EU) 2024/1624 (AMLR) on customer due diligence (CDD) and a mandate under Article 53(10) AMLD6 on pecuniary sanctions, administrative measures and periodic penalty payments.

4. In addition, the EC asked the EBA to consider possible guidance on the base amounts for pecuniary sanctions under Article 53(11) AMLD6 and on the minimum requirements for group-wide policies under Article 16(4) AMLR.

5. To the extent that this was possible, given its financial sector remit, the EC asked the EBA to highlight, in its response, which aspects of these instruments could also be relevant for the non-financial sector.

6. The EBA's response to the CfA will inform the work of the new Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA).

1.2 The EBA's proposals

1.2.1 Approach

7. The EBA's work on the CfA was guided by five principles:

   i. A proportionate, risk-based approach;

   ii. A focus on effective, workable outcomes;

   iii. Technological neutrality;

   iv. Maximum harmonisation across supervisors, Member States and sectors; and

v. Limiting disruption by building on existing EBA standards where possible, while aligning with global AML/CFT benchmarks.

8. To inform its approach, the EBA drew on findings from its prudential and AML/CFT work, including AML/CFT implementation reviews, the data collected through the AML/CFT database, EuReCA, ML/TF Risk Assessments, supervisory reporting and its monitoring of AML/CFT colleges. It assessed the impact and plausibility of its proposals using data from financial institutions and competent authorities and engaged closely with the EC, ESMA, EIOPA, the ECB and AMLA to ensure a consistent and joined-up approach. Throughout the life of the project, the EBA benefited significantly from the expertise and support of 60 EU competent authorities, which generously contributed their technical knowledge and resources.

9. In addition, the EBA engaged with the following stakeholders:

   i. The private sector and consumer groups through the EBA's Banking Stakeholder Group, a roundtable that took place on 24 October 2024 with 120 representatives from EU financial sector trade associations from all EU/EEA Member States and that was also hosted in parallel at national level by seven competent authorities, as well as bilateral meetings where this was necessary to obtain further information on specific sectors or practices.

   ii. The FIU Platform.

   iii. The European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB).

10. The EBA publicly consulted on a draft version of the four RTS under Articles 12(7) AMLAR, 40(2) AMLD6, 53(10) AMLD6 and 28(1) AMLR between 6 March and 6 June 2025, and conducted a public hearing in April 2025, which more than 600 stakeholders joined. 170 respondents provided written feedback.

11. The EBA did not consult publicly on its advice on possible guidance on the base amounts for pecuniary sanctions under Article 53(11) AMLD6 and on the minimum requirements for group-wide policies under Article 16(4) AMLR. This is because, in formulating this advice, the EBA drew only on information held by the EBA or contained in existing regulatory instruments.

1.2.2 The draft RTS on the assessment of the inherent and residual risk profile of obliged entities

12. Article 40 AMLD6 requires supervisors to apply a risk-based approach to AML/CFT supervision. Under a risk-based approach, supervisors have to adjust the frequency and intensity of supervision based on the ML/TF risk profile of each entity. This means that supervisors must understand the ML/TF risks present in their Member State, and how these

risks affect obliged entities within their scope in light of each entity's business model, operation and customer base.

13. Article 40, paragraph 2, AMLD6 requires AMLA to develop a common methodology that all supervisors will use to assess the level of ML/TF risks to which obliged entities under their supervision are exposed. As part of this, AMLA must set out in draft RTS how supervisors will assess and classify the inherent and residual risk profile of each obliged entity and the frequency at which such a risk profile must be reviewed.

Rationale

14. Findings from the EBA's AML/CFT implementation reviews, Opinions on ML/TF risk and a 2023 stocktake of supervisors' approaches to assessing entity-level ML/TF risk suggest that supervisors' approaches to assessing ML/TF risk vary significantly in terms of quality and scope. This can hamper AML/CFT supervision and undermine efforts to develop a common understanding of ML/TF risks at EU level, as results are not comparable. It also creates costs for financial institutions that operate on a cross-border basis. For example, feedback obtained by the EBA during its AML/CFT implementation reviews and the 2024 private sector roundtable suggests that divergent approaches by supervisors mean that financial institutions that operate on a cross-border basis have to report on the same risks in different Member States using different formats and timelines.

15. Considering these findings, the rationale underpinning the EBA's proposal is that supervisors' entity-level ML/TF risk assessment methodologies should be consistent across Member States, with comparable outputs going forward. They should reliably inform supervisors' strategies and inspection plans and help them target their resources on institutions that present the highest ML/TF risks. The proposed approach should also ensure that the cost of compliance with the new requirements does not exceed what is strictly necessary to achieve this goal.

EBA advice

16. The EBA's proposal for a draft RTS is contained in Section 2.1 of this report.

Overview of the scoring system

17. **The methodology proposed by the EBA comprises three steps**. They include:

    i. An assessment of each obliged entity's level of exposure to inherent ML/TF risks. The inherent risk profile of each obliged entity should be classified into one of the following inherent risk categories on the basis of this assessment: low risk (1), medium risk (2), substantial risk (3), or high risk (4).

    ii. An assessment of the quality of the AML/CFT controls put in place by the obliged entity to address these risks. The obliged entity should be classified into one of the following controls categories on the basis of this assessment: very good quality of controls (A),

good quality of controls (B) moderate quality of controls (C), or poor quality of controls (D).

iii. An assessment of the level of exposure to ML/TF risks to which the obliged entity remains exposed after taking into account the quality of its AML/CFT control framework. The obliged entity should be classified into one of the following residual risk categories on the basis of this assessment: low risk (1), medium risk (2), substantial risk (3) or high risk (4).

18. **The residual risk score represents the level of risk that remains after controls have been applied**. This is in line with the Financial Action Task Force (FATF)'s approach and means that the residual risk score cannot be greater than the inherent risk score. At the same time, poor controls may attract higher risk customers over time, leading to an increase in an institution's inherent risk exposure. To ensure that supervisors have sight of risks associated with a poor or absent controls environment, and can plan their supervisory response accordingly, the EBA proposes that the residual risk score be displayed as a matrix (Figure 1).

			Inherent Risk															
			1				2				3				4			
Controls			1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.60	2.80	3.00	3.20	3.40	3.60	3.80	4.00
	D	4.00	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.60	2.80	3.00	3.20	3.40	3.60	3.80	4.00
		3.80	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.60	2.80	3.00	3.20	3.40	3.60	3.80	3.90
		3.60	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.60	2.80	3.00	3.20	3.40	3.60	3.70	3.80
		3.40	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.60	2.80	3.00	3.20	3.40	3.50	3.60	3.70
	C	3.20	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.60	2.80	3.00	3.20	3.30	3.40	3.50	3.60
		3.00	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.60	2.80	3.00	3.10	3.20	3.30	3.40	3.50
		2.80	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.60	2.80	2.90	3.00	3.10	3.20	3.30	3.40
		2.60	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.60	2.70	2.80	2.90	3.00	3.10	3.20	3.30
	B	2.40	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.40	2.50	2.60	2.70	2.80	2.90	3.00	3.10	3.20
		2.20	1.00	1.20	1.40	1.60	1.80	2.00	2.20	2.30	2.40	2.50	2.60	2.70	2.80	2.90	3.00	3.10
		2.00	1.00	1.20	1.40	1.60	1.80	2.00	2.10	2.20	2.30	2.40	2.50	2.60	2.70	2.80	2.90	3.00
		1.80	1.00	1.20	1.40	1.60	1.80	1.90	2.00	2.10	2.20	2.30	2.40	2.50	2.60	2.70	2.80	2.90
	A	1.60	1.00	1.20	1.40	1.60	1.70	1.80	1.90	2.00	2.10	2.20	2.30	2.40	2.50	2.60	2.70	2.80
		1.40	1.00	1.20	1.40	1.50	1.60	1.70	1.80	1.90	2.00	2.10	2.20	2.30	2.40	2.50	2.60	2.70
		1.20	1.00	1.20	1.30	1.40	1.50	1.60	1.70	1.80	1.90	2.00	2.10	2.20	2.30	2.40	2.50	2.60
		1.00	1.00	1.10	1.20	1.30	1.40	1.50	1.60	1.70	1.80	1.90	2.00	2.10	2.20	2.30	2.40	2.50

Figure 1: Example of a matrix that can be used to display the residual risk score. A matrix allows supervisors to distinguish between institutions that have the same residual risk rating (e.g. 2.0) but effective controls to mitigate high inherent risk (e.g. 3A), or poor controls that are insufficient to mitigate lower levels of inherent risk (e.g. 2D)

Sources of information

19. **The EBA proposes that the assessment of inherent risks and the quality of controls be performed using a common set of data points and a common, automated, scoring system.** To ensure a consistent approach and comparable outcomes, adjustments are subject to specific rules and limits and possible only on the basis of evidence. Competent authorities would be able to adjust:

i. The overall inherent risk score by one category to the extent that this is necessary to reflect specific national risks or insights obtained in the context of onsite or offsite supervision.

ii. The scores assigned to control components based on qualitative information acquired in the context of on- or offsite supervision or external auditors' assessments.

20. The EBA proposes that:

a. **The draft RTS introduce a single set of data points that all supervisors would be required to use to establish the indicators**. An interpretive note should accompany the draft RTS and clarify the meaning of these data points so that they are understood in the same manner in all Member States and by all obliged entities (see Annex 2).

b. **The draft RTS do not specify how supervisors collect these data points, because the relevant sources of information may vary from one Member State to another**. For instance, in some cases, supervisors may be able to collect information from their prudential counterparts or from the local FIU, while in other cases they will need to collect all the data from the obliged entities.

c. **The same set of data points and scoring system is used to assess ML and TF risks**. This is because the purpose of the risk assessment methodology is to reflect obliged entities' overall level of exposure to both types of risks, in a way that allows supervisors to compare and rank them.

d. **Quantitative and objective data are used where possible**. Consequently, the proposed methodology does not envisage reliance on a self-assessment by obliged entities of the level of ML/TF risks to which they are exposed.

Keeping risk assessments up to date

21. **Because risks vary and evolve, specific scoring thresholds and weights are not included in the draft RTS**. Instead, it would be the role of AMLA to define the specific scoring thresholds and weights for each review cycle and to monitor the effective application of these indicators by supervisors in all Member States.

22. **The draft RTS adjust the frequency of entity-level risk assessments based on the nature and size of financial institutions**. To have an up-to-date understanding of the risks to which obliged entities under their supervision are exposed, and in line with most national supervisors' current practices, supervisors would review the inherent and residual risk profile of obliged entities once per year unless an institution is small or carries out activities that do not justify a yearly review. In such cases, a review would take place once every three years instead. However, supervisors would be expected to review an entity's risk profiles

and, if necessary, obtain risk assessment data more frequently should risks crystallise or new information emerge that suggests that the ML/TF risk profiles may no longer be accurate.

23. The draft RTS do not prevent supervisors from collecting information from obliged entities for other purposes, such as offsite supervision.

Application to non-financial sector obliged entities

24. The EBA's proposals apply to AML/CFT supervisors of credit and financial institutions. However, Article 40(2) AMLD6 applies to all obliged entities, including those operating in the non-financial sector. Following consultation with the EC's non-financial sector expert group, provisions in Articles 1 to 4 of the draft RTS appear to be relevant for the non-financial sector to some extent.

25. The data points included in Annex 1 will not be relevant for non-financial sector entities who should benefit from an adapted list of data points that is specific to their sectors. The provisions governing the frequency of review (Article 5 of the draft RTS) should also be adapted to such entities, based on an assessment of the size and nature of their business, in accordance with Article 40(2) AMLD6.

26. To ensure the effective implementation of the methodology and a proportionate approach, the EBA also recommends that AMLA develops separate RTS for the financial and non-financial sectors. This approach would allow the financial sector and its AML/CFT supervisors to progress swiftly under the new framework and strengthen the EU's AML/CFT defences. It would also give AMLA time to consult with the non-financial sector and build a robust approach based on evidence that can be implemented effectively by entities to which it is addressed.

1.2.3 The draft RTS on risk assessment for the purpose of the selection of credit institutions, financial institutions and groups of credit and financial institutions for direct supervision

27. Article 5(2) AMLAR requires AMLA to supervise selected obliged entities that are credit institutions, financial institutions and groups of credit and financial institutions. Article 12 AMLAR defines the selection process.

28. According to Article 12(1) AMLAR, credit institutions, financial institutions and groups of credit and financial institutions that are operating in at least six Member States, including the home Member State, are eligible to be directly supervised by AMLA, whether through freedom of establishment or the freedom to provide services.

29. AMLA will then select which of these institutions it will directly supervise, taking into account their residual ML/TF risk profile.

30. A mandate under Article 12(7) AMLAR requires AMLA to specify:

a. how to determine the number of Member States in which an obliged entity operates either via establishments or via the freedom to provide services, by defining the minimum activities obliged entities need to carry out under the freedom to provide services to be considered as 'operating in a Member State other than that where it is established' (Article 12(7)(a) AMLAR); and

b. how to determine the level of risk of each eligible entity, by defining the methodology for classifying the inherent and residual ML/TF risk profiles of an obliged entity as low, medium, substantial or high (Article 12(7)(b) AMLAR).

Rationale

31. The establishment of an EU AML/CFT authority with direct supervision powers over some obliged entities constitutes a significant departure from the current regime, where AML/CFT supervision is performed solely by national supervisors. Nevertheless, under the new legal and institutional framework, national and supranational approaches remain closely intertwined. Accordingly, Recital (21) AMLAR states that, where appropriate, AMLA should ensure alignment between the methodology for the ML/TF risk assessment at national level and the methodology for selection.

32. When formulating its proposals, the EBA had due regard to the intention, among the co-legislators, that AMLA provide consolidated AML/CFT oversight of high ML/TF risk institutions operating across multiple EU jurisdictions. It also considered the need for specific measures to support the smooth transition to the new ML/TF risk assessment framework.

EBA advice

33. The EBA's proposal for draft RTS is contained in Section 2.2 of this report

Determining which entities are eligible for direct supervision

34. **The EBA proposes that, when determining which institutions are eligible for direct AML/CFT supervision in principle, AMLA distinguishes between situations where the free provision of services is to be considered material, and situations where it is not.** A key feature of the freedom to provide services is the possibility of entering new markets without incurring the administrative and financial commitment that setting up an establishment entails. As a result, obliged entities often notify their intention to operate in another Member State through the freedom to provide services, but do not provide services in that Member State. Obliged entities may also provide services in a Member State in a way that is not material.

35. **In line with the scope of the mandate in Article 12(7)a AMLR, the draft RTS do not provide a definition of the freedom to provide services or the type of activities that fall within the scope of free provision of services**. Instead, they clarify whether an entity should be

considered as operating in a certain Member State where it is not established for the purposes of Article 12(1) AMLAR.

36. Considering the above, **the draft RTS establish thresholds for determining whether operations under the freedom to provide services in a Member State are sufficiently material to consider an entity as operating in that Member State for the purposes of Article 12(1) Article 12(1) AMLAR.** These thresholds are based on: (i) the number of customers that are resident in the relevant Member State where the obliged entity is operating under the freedom to provide services, which must be equal to or greater than 20 000; (ii) the total value in euro of incoming and outgoing transactions generated by customers that are resident in the relevant Member State, which must be equal to or greater than EUR 50 000 000.

37. **The EBA proposes to use the number of customers that are resident in the Member State where the entity is operating under the freedom to provide services as a proxy.** This is because feedback from private sector representatives suggests that identifying customers that have been acquired under the freedom to provide services could be burdensome, as most institutions are not able to provide a breakdown of all customers onboarded under freedom to provide services for each Member State of operation. Regarding the volume of transactions, the aim of having such a threshold is to capture situations where the number of customers that are resident in a certain Member State is limited but where these customers generate a high volume of transactions.

38. **These thresholds are alternative**. This means that it is sufficient for an obliged entity to meet just one threshold to be considered as having a material operation under the freedom to provide services in a certain Member State.

Determining which entities will be selected for direct supervision

39. **The EBA proposes that the methodology for the risk assessment of eligible credit institutions and financial institutions under Article 12(7)(b) AMLAR build on the methodology for entity-level risk assessment under Article 40(2) AMLD6**. Using the same methodology for both risk assessments limits the operational burden on the obliged entities and on supervisors that divergent approaches would entail. It will also make the operation of the EU's AML/CFT supervisory system more efficient.

40. **The EBA considers that, for the purposes of Article 12(7)b AMLAR, adjustments of entity-level ML/TF risk scores should be limited to prevent arbitrage.** One of the key objectives of the selection methodology is to ensure a level playing field. Therefore, the possibility of adjusting the inherent risk score based on national specificities, or other considerations identified by supervisors that exist within the methodology for entity-level risk assessment under Article 40(2) AMLD6, has been excluded from the methodology for the risk assessment of eligible credit institutions and financial institutions under Article 12(7)(b) AMLAR.

41. **The draft RTS also include a methodology for calculating the group-wide ML/TF risk score**. This methodology is based on an aggregation of entity-level residual risk scores and consists of a weighted average that reflects the importance of each entity within the group. The intention is to give due consideration to entities that carry a high ML/TF risk, operate in riskier sectors, and whose operations represent a sizeable part of the group's overall operations. It is to avoid lower-risk entities unduly lowering the group's overall ML/TF risk score.

Ensuring a smooth transition

42. To ensure a smooth transition to the new approach, **the EBA proposes that the provisions of the draft RTS under Article 40(2) on the determination of the inherent and residual risk profile of obliged entities be reproduced in the draft RTS under Article 12(7).** This is because different deadlines apply for the publication of the draft RTS under Article 12(7) AMLAR (i.e. 1 January 2026) and the draft RTS under Article 40(2) AMLD6 (10 July 2026) for the RTS under Article 40(2) AMLD6. If the provisions under Article 40(2) AMLD6 were not reproduced in Article 12(7) AMLAR, there would be a risk that the methodology for entity-level risk assessment under Article 40(2) AMLD6 would not yet be legally binding in all Member States when the methodology for the risk assessment of eligible credit institutions and financial institutions under Article 12(7)(b) AMLAR is applied for the first time. This would undermine the effectiveness of the first selection process and could mean that the high-risk credit institutions and financial institutions are not identified or selected.

43. **In addition, some data points will only apply at a later stage.** Pursuant to Article 13(4) AMLAR, the first selection process must start on 1 July 2027. This means that, for the purpose of this first selection process, AMLA will need to base its assessment on data relating to the year 2026. This leaves limited time for the private sector to adapt to new reporting requirements. Feedback from the private sector suggests that two data points are particularly challenging in this regard:

    a. The inherent risk data point 'Number of customers with high-risk activities' may be difficult to provide in a consistent way for the year 2026 as there is no comprehensive EU list of high-risk economic activities and sectors that could currently be used to classify customers based on their activity. The risk assessment at Union level, to be published by the EC pursuant to Article 7 AMLD6 is likely to contain useful information in this regard. Consequently, this data point should be introduced at a later stage, and it should not apply to the first selection process.

    b. The controls quality data point 'Number of customers whose CDD data and information is not yet in line with the requirements of Article 20 AMLR' cannot be implemented in the 2026 period because it refers to Article 20 AMLR, which will apply only from 10 July 2027.

44. **Finally, the EBA proposes that, for the purpose of the first selection, AMLA base its assessment of the quality of controls on the automated score resulting from the**

application of the methodology. Because national approaches currently diverge, including the supervisory judgement in the calculation of the ML/TF controls quality score from the start could affect the comparability of the scores and, ultimately, the results of the first selection itself. For this reason, during the transition period and until the single supervisory handbook, under Article 8 AMLD6, is in force, manual, supervisory judgement-based adjustments of controls risk scores that are possible in line with the proposed methodology should only be possible in exceptional circumstances.

Application to the non-financial sector

45. Article 12(7) AMLAR does not apply to the non-financial sector.

1.2.4 The draft RTS on Customer Due Diligence

46. Article 28(1) AMLR requires AMLA to harmonise customer due diligence requirements by specifying, by means of draft RTS, which information obliged entities must collect to perform standard customer due diligence (CDD), simplified due diligence (SDD) and enhanced due diligence (EDD). AMLA must also set out in the draft RTS which reliable and independent sources of information obliged entities may use to verify the identity of natural or legal persons for the purposes of Article 22(6) and (7) AMLR.

47. The mandate in Article 28(1) AMLR also covers the risk factors associated with features of electronic money instruments that should be taken into account by supervisors when determining the extent of the exemption for electronic money under Article 19(7) AMLR, and the list of attributes which electronic identification means and relevant qualified trust services referred to in Article 22(6), point (b), AMLR must feature in order to fulfil the requirements of Article 20(1), points (a) and (b), AMLR.

48. The scope of the mandate in Article 28(1) AMLR is strictly defined. It also interacts with other AMLR articles and mandates, particularly Articles 20(2) and (3) and 28(2) on customer risk assessments, Chapter IV on beneficial ownership transparency, and Article 26(5) on transaction monitoring.

49. The EC did not ask the EBA for advice on these articles or mandates. It will fall to AMLA, as it progresses its work on the remaining AML/CFT instruments, to ensure that the final regulatory framework is coherent and can be applied effectively.

Rationale

50. CDD is central to obliged entities' AML/CFT efforts. Under the current framework, differences in the national transposition of the CDD requirements in Directive (EU) 2015/849 and, as a result, divergent expectations of obliged entities' CDD efforts by supervisors have led to regulatory arbitrage, created uneven competition conditions and hampered innovation and the cross-border provision of financial services. They also exposed the EU's financial sector to ML/TF risk. To address this, the AMLR introduces a single AML/CFT rulebook that sets out in detail what obliged entities in all Member States

must do to comply. It therefore constitutes a significant departure from current EU AML/CFT practices.

51. The scale of change introduced by the AMLR could create ML/TF vulnerabilities during a transition phase as institutions adjust their AML/CFT systems and controls to comply with the new requirements. To mitigate this risk, where possible and to the extent that this was justified by effective outcomes, the EBA decided to build on and align with existing EBA works and standards, such as the EBA's Guidelines on ML/TF risk factors, the EBA Guidelines on remote customer onboarding and the EBA Guidelines on the implementation of EU and national restrictive measures.

EBA advice

52. The EBA's proposal for draft RTS is contained in Section 2.3 of this report.

53. **The EBA proposes that the structure of the draft RTS follows the sequencing of the mandate to facilitate its application by obliged entities.** As a result, the proposed draft RTS focus first on the CDD, SDD and EDD measures obliged entities must take, then on the ML/TF risk factors associated with features of electronic money instruments that should be taken into account by supervisors and, finally, on the list of attributes which electronic identification means and relevant qualified trust services must feature in order to fulfil the requirements of Article 20(1), points (a) and (b), AMLR, in the case of CDD, SDD and EDD.

54. **The EBA advocates for a principles-based, risk-based approach that focuses on effective outcomes where this is warranted and to the extent that the Level 1 requirements permit it**. When drafting the RTS on CDD, the EBA consulted with private sector representatives to understand the impact the new CDD requirements would have on their businesses and operations. Representatives suggested that the AMLR's CDD requirements will have a significant impact. They also said that the detailed requirements of the AMLR and a prescriptive, rules-based approach to discharging the mandate in Article 28(1) AMLR could further increase the cost of compliance without tangible benefits. To address these concerns, the EBA proposes that the draft RTS remain silent where sufficient detail is provided in the AMLR. The EBA also proposes that, where possible and desirable in terms of the overall outcomes, the draft RTS do not list specific documents but adopt a principles-based approach in relation to the type and source of information to be collected by obliged entities. The EBA introduced additional provisions after the public consultation to strengthen the risk-based approach further.

55. **The scale of change introduced by the AMLR makes transition provisions necessary.** In relation to the date on which obliged entities are expected to comply with the CDD measures set out in the AMLR, the AMLR could be read as suggesting that obliged entities will have to comply with as from 10 July 2027. This would mean that obliged entities would have to apply these CDD standards to all existing customers on that date. The EBA acknowledges that it may not be possible for obliged entities to apply the new CDD standards to all of their existing clients on that date. The draft RTS therefore clarify that

obliged entities apply a risk-based approach. Specifically, when updating CDD information for existing customers, obliged entities would prioritise higher ML/TF risk business relationships in the first instance. CDD information for other business relationships, which are not high ML/TF risk, could be completed within a 5-year transition period unless there is a trigger in the customer identification data which necessities an earlier update. Last but not least, the EBA confirms that the RTS on CDD will not be applicable earlier than the AMLR's application date.

Application to the non-financial sector

56. CDD is key to fighting financial crime and applies to all obliged entities within the scope of the EU's AML/CFT framework. Several of the provisions set out in the proposed RTS apply to obliged entities in the non-financial sector in the same way as institutions in the financial sector. Sections 1–7 and Section 9 of the draft RTS under Article 28(1) AMLR are likely to be relevant.

57. At the same time, the diverse nature of entities in the non-financial sector means that some aspects of these RTS may need to be tailored to specific business models to avoid unnecessary costs and ensure an effective approach. It will fall to AMLA to determine where this might be the case.

58. Overall, considering the significant differences between the financial and non-financial sectors in terms of business models, operation, AML/CFT capacity and compliance maturity, AMLA may wish to assess the need for separate, standalone RTS on CDD measures for the non-financial sector. Tailored RTS could also support the adoption of effective AML/CFT controls by the obliged entities from the non-financial sector, listed under Article 3 AMLR, which are newly designated obliged entities, with no or limited experience of AML/CFT-related rules.

1.2.5 The draft RTS on pecuniary sanctions, administrative measures and periodic penalty payments

59. The mandate in Article 53(10) AMLD6 covers three aspects: (i) indicators to classify the level of gravity of breaches, (ii) criteria to be taken into account when setting the level of pecuniary sanctions or applying administrative measures and (iii) the methodology for the imposition of periodic penalty payments (PePPs).

Rationale

60. The draft RTS comply with the principle stipulated by the AMLD6 that pecuniary sanctions, administrative measures and PePPs may be imposed separately or in combination. It aims to achieve the highest possible level of harmonisation to ensure that the same breach of AML/CFT requirements is assessed in the same way by all supervisors in all Member States and that the resulting enforcement measure is proportionate, effective and dissuasive.

61. The EBA first stressed the importance of a proportionate, effective, dissuasive and harmonised approach to enforcement in its 2020 response to the EC's Call for Advice on the future AML/CFT framework. Progress since then has been limited. For example, the fourth round of the implementation reviews carried out by the EBA in 2023/2024[2] showed that, while national supervisors assessed during that round had taken steps to strengthen their approach to enforcement, enforcement measures did not always constitute a deterrent, and not all supervisors were using their powers effectively. Moreover, while most supervisors had taken some enforcement actions, it was not always clear on what basis they had selected the supervisory or administrative measures and how they had calculated the value of the fine: this was because more than half of all supervisors in this round did not have a comprehensive internal enforcement and sanctioning policy or procedures in place.

62. The need to ensure convergence is further highlighted by the data collected in EuReCA, the EBA's AML/CFT database, which contains information on serious deficiencies identified in financial institutions[3]. Since its launch in 2022, competent authorities have submitted over 1,200 corrective measures that they have applied to remediate or enforce against financial institutions for material breaches of their AML/CFT obligations. Information provided by supervisors as part of these reports shows that approaches to enforcement are not aligned. For example, although differences in the level of fines or other enforcement measures are expected, given the range of financial institutions and differences in the severity of individual findings, EuReCA data suggest that similar breaches by financial institutions in similar situations currently result in different supervisory responses.

63. EuReCA data also highlight the need to address sanctions for natural persons. Since May 2024, when competent authorities started to report information concerning natural persons, 21 subjects have been mentioned.

64. Finally, when considering provisions regarding PePPs, the EBA had due regard to PePPs being an enforcement measure and not a pecuniary sanction, because their aim is to incite the obliged entity to take action to comply with administrative measure(s). This means that the criteria used by supervisors before deciding on the amount of the PePP should not be the same as the criteria proposed for the imposition of pecuniary sanctions.

EBA advice

65. The EBA's proposal for draft RTS is contained in Section 2.4 of this report.

66. **The approach proposed by the EBA consists of several consecutive steps**:

[2] Report on NCA's approaches to the supervision of banks with respect to Anti-Money Laundering and Countering the Financing of Terrorism (round 4 – 2023/4).

[3] Central database of AML/CFT related information collected by the EBA pursuant to Article 9a (2) of Regulation (EU) No 1093/2010 and Commission Delegated Regulation (EU) 2024/595 (see Factsheet on EuReCA).

a. **As a first step, supervisors will assess the level of gravity of a breach**. To ensure a consistent approach, the draft RTS set out a list of indicators that all supervisors will take into account. These indicators reflect policy work already done by the EBA to the extent possible, including the RTS on the central AML/CFT database (EuReCA)[4] and the Joint ESAs Report on the withdrawal of authorisation for serious AML/CFT breaches[5].

b. **In a second step, supervisors will classify the level of gravity of a breach in one of four categories by order of severity**. The RTS set out how breaches should be classified into each of those categories. A breach with a level of gravity classified as category three or four shall be deemed serious, repeated or systematic within the meaning of Article 55(1) of Directive (EU) 2024/1640 and will trigger the application of a pecuniary sanction.

c. **In a third step, supervisors determine the level of pecuniary sanctions or administrative measures.** The RTS list the criteria supervisors will apply to this effect. For administrative measures, the RTS focus on the most severe measures listed in Article 56(2) AMLD6 (i.e. point (f) withdrawal or suspension of authorisation, point (e) restriction or limitation of business, and point (g) change in governance structure), in order to foster convergence in enforcement activities related to the most serious breaches.

67. **The EBA considers that, for enforcement to be proportionate and effective, supervisors must take into account the context in which the breach has occurred.** This means that a tick-box approach is not warranted. Instead, supervisors must apply supervisory judgement to determine whether and to what extent different indicators and criteria are met. To make this possible, the lists of indicators and criteria included in the draft RTS are non-exhaustive. Similarly, while specific combinations of indicators should be classified in specific categories, supervisors may use these categories for other combinations of indicators also.

68. **The draft RTS contain specific provisions for natural persons,** including senior management and the management body in its supervisory function. EU trade association representatives suggested during the EBA roundtable in October 2024, and subsequently in their responses to the public consultation, that holding individuals accountable for AML/CFT failures is an important deterrent and, in their view, an essential part of effective enforcement.

69. **Cooperation with prudential supervisors is important, but it is not part of the mandate of Article 53(10) AMLD6.** AMLA will have the opportunity to include such provisions in a future RTS under Article 53(9) and Article 55(5) AMLD6 and the provisions contained in Articles 44 to 51 AMLD6.

[4] Commission Delegated Regulation (EU) 2024/595, OJ L, 2024/595, 16.2.2024.

[5] ESAs 2022/23, 31 May 2022, Joint ESAs report.

70. **The general principles of administrative law, including the principle of non-self incrimination, proportionality and fairness, apply to all Union acts and to any enforcement proceedings**. This means that they apply to these RTS and do not have to be set out specifically.

Periodic Penalty Payments (PePPs)

71. Where possible, the EBA's proposed approach to PePPs aligns with delegated acts issued by the EC and the practice of Member States in which they are already applied. It covers procedural aspects for the imposition of PePPs, e.g. the right to be heard, a limitation period for the collection of PePPs, and the minimum content of the decision by which a PePP is imposed. It reiterates that, unless otherwise stipulated, the PePPs imposition process shall be governed by national law in force in the Member State where the PePPs are imposed and collected.

Transition

72. A transition provision reduces the risk of divergent applications of the provisions by different supervisors. The provision establishes a cut-off date, 10 July 2027, until which national rules for ongoing proceedings shall apply. This date matches the date by when the provisions of the AMLD6 shall be transposed into Member States' legal orders. For proceedings initiated on or after 10 July 2027, the provisions of the draft RTS shall apply.

73. Though not stipulated in the draft RTS, considering the scale of the changes introduced by these RTS, given the absence of a previously established EU-wide enforcement framework, the consistent implementation of this new common framework across Member States could be supported by the exchange of practical experience gained from applying the RTS at both EU and national levels, for example through a network of enforcement practitioners. Going forwards, to ensure convergence of practices, additional guidance could be considered.

Application to the non-financial sector

74. The EBA included in the consultation a specific question on the applicability of the RTS indicators and criteria to the non-financial sector. Several respondents highlighted that the non-financial sector should be subject to the same stringent enforcement measures as the financial sector, to mitigate the ML/TF risk emanating from this sector. Most respondents also considered that the RTS indicators and criteria were relevant to the non-financial sector, with limited exceptions connected mostly to the specificities of some business models. To ensure proportionality, fairness, flexibility and adaptability of the related framework to the non-financial sector, NCAs should, for instance, pay attention to the following aspects:

    a. The size, structure and type of business;

b. capital or liquidity requirements, as they may not apply to non-financial sectors;

c. indicators that relate to the cross-border impact of a breach, as obliged entities from the non-financial sector do not operate across jurisdictions in the same manner as obliged entities from the financial sector.

1.2.6 Technical advice on base amounts for pecuniary fines under Article 53(11) AMLD6

75. Pursuant to Article 53(11) AMLD6 AMLA must issue, by 10 July 2026, guidelines on the base amounts for the imposing of pecuniary sanctions relative to turnover, broken down per type of breach and category of obliged entities.

76. The EC asked the EBA to propose options that AMLA should consider when taking the mandate forward and, where possible, to advise AMLA on the options it should take forward.

Rationale

77. The main policy objective of the guidelines on base amounts is to create a harmonised approach that would help supervisors determine the base amount for breaches of AML/CFT obligations, thus ensuring that similar breaches committed by specific categories of obliged entities would be treated in a comparable way within the Member States of the European Union.

EBA advice

78. The EBA's analysis of options AMLA may wish to consider is contained in Section 3.1 of this report.

79. Regarding the scope of the guidelines, and having assessed different options, the EBA considers that these guidelines should (i) apply both to NCAs and to AMLA, (ii) cover all breaches applicable to obliged entities, (iii) address breaches committed by obliged entities that are legal persons, natural persons, members of senior management and other natural persons who under national law responsible for the breach of obligations stipulated by the AML/CFT framework, and (iv) be consistent with the future RTS on pecuniary sanctions.

80. The EBA considers that some of the terms used in the mandate should be defined to ensure a common interpretation by all competent authorities. This is the case, in particular, for the terms (i) base amounts, (ii) type of breach, (iii) category of obliged entity, and (iv) turnover.

81. Regarding the application of these guidelines, as is the case for the draft RTS on sanctions, the EBA considers that these guidelines should apply from 10 July 2027, which is the date by when MSs are obliged to transpose the provisions of the AMLD6 into their national legal system.

Application to the non-financial sector

82. The scope of the mandate included in Article 53(11) AMLD6 extends to all categories of obliged entities, including the non-financial sector.

83. In the case of non-financial sector, AMLA will need to have due regard to differences in the way maximum thresholds for imposing pecuniary sanctions are drafted in Articles 55(2) and 55(3) AMLD6.

84. It will also have to take into account the specificities of entities in the non-financial sector regarding, for example, their business models, size, turnover and customer base to ensure the application of the principle of proportionality.

1.2.7 Technical advice on group-wide policies and procedures

85. Article 16(4) AMLR requires AMLA to draft RTS defining the minimum standards for information-sharing within the group, criteria for identifying the parent undertaking and conditions for applying group-wide obligations to entities with shared ownership, management or compliance control.

86. The EC asked the EBA to propose options that AMLA could consider when taking this mandate forward to the extent possible with the resources the EBA had available.

Rationale

87. Effective information within a group supports the identification of ML/TF risks and makes effective group-wide AML/CFT supervision possible. Information that should be shared includes personal information as a prerequisite for obtaining a single customer view – a consolidated profile that enhances transaction monitoring and customer risk assessments across the group. This must be subject to strict data protection safeguards.

EBA advice

88. The EBA's analysis of options considered is contained in Section 3.2 of this report. It focuses on aspects related to the sharing of information within a group.

89. In its advice, the EBA proposes that EU standards that govern how information is shared within a group specify which information should be shared and what acceptable uses of such information entail. They should also consider how such information should be shared.

90. Regarding the type of personal information that should be shared, the EBA advises that a broad definition be adopted. An institution that is part of a group should have access to all information that group entities hold on their customer, including information on suspicious activities or transactions, as well as aggregated data, typologies and trends. At the same time, it is important that access to information held by another group entity does not lead

to unwarranted de-risking. This could be the case, for example, where another group entity classifies a customer as high ML/TF risk, or because they have named them in an STR.

91. In respect of the acceptable uses of personal information obtained in the group context, the EBA advises that this be linked to ML/TF risk assessments of customers, the entity's business and the group's operations. Acceptable uses also include the onward sharing of information obtained through membership of a partnership for information-sharing, if specific conditions are met.

92. Fulfilling the mandate in Article 16(4) AMLR also means that consideration should be given to how information is shared, for example through specific structures, or provisions governing the sharing of information in specific situations. The role of the parent undertaking is important, as are provisions to ensure that personal data are protected. This will be particularly important where sensitive data are shared with entities of the group that are based in third countries.

93. Finally, the EBA notes that several aspects that are relevant for the effective discharge of the mandate under Article 16(4) AMLR interact with provisions in prudential regulations and with other AMLA mandates under the AML/CFT package. AMLA's approach to drafting these RTS should complement those provisions to ensure that the resulting framework is consistent and can be applied effectively by all institutions that are members of a group.

Application to the non-financial sector

94. This advice applies to the financial sector as it does to the non-financial sector.

2. Draft regulatory technical standards

2.1 Draft RTS on the assessment of the inherent and residual risk profile of obliged entities under Article 40(2) of Directive (EU) 2024/1640

COMMISSION DELEGATED REGULATION (EU)
No …/..

of XXX

supplementing Directive (EU) 2024/1640 of the European Parliament and of the Council with regards to regulatory technical standards setting out the benchmarks and methodology for assessing and classifying the inherent and residual risk profile of obliged entities, as well as the frequency at which it shall be reviewed

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024, on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and in particular Article 40, paragraph 2, thereof,

Whereas:

(1) Directive (EU) 2024/1640 sets out the obligation for Member States to ensure that competent authorities apply a risk-based approach to supervision. As part of this, competent authorities should identify and assess the ML/TF risks to which obliged entities are exposed, as a result of the characteristics of their customers, the types of products, services or transactions they offer, the jurisdictions in which they operate and the distribution channels that they use.

(2) Pursuant to Article 40(2) of Directive (EU) 2024/1640, AMLA is mandated to develop benchmarks and a methodology to ensure that the inherent and residual risk profiles of individual obliged entities can be assessed and classified in a consistent manner by all competent authorities.

(3) To ensure that the risk profile of obliged entities is assessed and classified in a consistent manner across the Union, the assessment and classification of the inherent and residual risk profile of obliged entities should be conducted on the basis of the same information in all Member States.

(4) This Regulation does not specify how competent authorities should obtain the information on which the assessment should be based. Supervisors may collect relevant data from different sources, either from the obliged entities themselves, from external auditors, or from AML/CFT authorities, prudential supervisors, FIUs or other public bodies in the context of cooperation or ongoing exchanges. Supervisors should use these data to establish a set of harmonised indicators. These indicators should be scored using the same methodology and combined using the same weighting system to determine the inherent and residual risk profile of obliged entities.

(5) Article 40, paragraph 2, of Directive (EU) 2024/1640 requires supervisors to assess and classify both the inherent and residual risk profiles of obliged entities. Consequently, supervisors should adopt a three-step approach. Firstly, supervisors should assess and classify the inherent risk profile of obliged entities based on a set of indicators aimed at reflecting the level of ML/TF risks to which they are exposed. Secondly, supervisors should assess the quality of the AML/CFT controls put in place by obliged entities to mitigate the inherent ML/TF risks to which they are exposed. Lastly, supervisors should assess and classify the residual risk profile of obliged entities which should reflect the level of ML/TF risk to which obliged entities remain exposed after their controls have been applied.

(6) Inherent ML/TF risks can stem from different types of risk factors, namely factors relating to the nature of customers, factors relating to the nature of the services, products or types of transactions offered, factors relating to the distribution channels used, and factors relating to the geographical areas in which obliged entities are operating. To structure the assessment of inherent risks, the inherent risk indicators should therefore each be divided into four categories reflecting the different types of risk factors and controls mentioned above. Moreover, within certain categories, some indicators relate to the same topic and should therefore be grouped into sub-categories. Similarly, different types of AML/CFT controls can be identified. To structure the assessment of the quality of controls, these different indicators should also be classified into different categories corresponding to these different types of controls.

(7) Indicators comprising a sub-category or category will generally not have the same level of significance. Consequently, indicators should be given different weights in the determination of the combined score attributed to this sub-category or category. Equally, the sub-categories comprising a category may have different levels of significance and should also be given different weights in the determination of the combined score per category.

(8) Some sectors have specificities that affect the level of ML/TF risks to which the obliged entities operating in these sectors are exposed. These specificities should be reflected in the methodology by adjusting the list of applicable indicators and the weights given to these indicators, depending on the sector(s)

to which the assessed obliged entities belong. The assessment of the risks of money laundering and terrorist financing and of non-implementation and evasion of targeted financial sanctions affecting the internal market and relating to cross-border activities conducted by the Commission pursuant to Article 7 of Directive (EU) 2024/1640 should be used as a source of information to determine the extent to which adjustments are needed for the different sectors.

(9) Similarly, supervisors may possess relevant information suggesting that the obliged entity's inherent risk score does not reflect the level of inherent ML/TF risks to which it is exposed, for instance due to national specificities of their Member States. This information should be reflected in the methodology by introducing a mechanism whereby supervisors can adjust the inherent risk score of the relevant obliged entities, based on duly justified considerations.

(10) ML/TF risks affecting the internal market are constantly evolving. It is therefore important that the methodology can be adjusted on an ongoing and timely basis to capture these evolutions. To ensure that this is possible, the precise values and thresholds to be applied to score each indicator and the precise weights to be given to each indicator, sub-category and category in the determination of the inherent and residual risk profile of obliged entities should not be specified in this Regulation. It will be the role of AMLA to develop and keep up to date the necessary guidance to ensure that each competent authority applies the same thresholds and weights.

(11) To ensure that supervisors' understanding of the ML/TF risks to which obliged entities are exposed, the inherent and residual risk profile of obliged entities should be reviewed at least once per year. Where the size of the business of an obliged entity is very small, or where the nature of the business exposes the entity to a low level of risk or does not justify reviewing the inherent and residual risk profile of the obliged entity every year, supervisors should be able to review such profile only once every three years, provided that no major event or development in the management and operations of the relevant obliged entity occurs during the three years preceding the assessment.

(12) Major events or developments in the management and operations of obliged entities can significantly affect the ML/TF risks to which the relevant obliged entities are exposed, in a way that justifies a rapid supervisory reaction. Where such events or developments occur, supervisors should conduct an ad hoc assessment of the impact of those events or developments on the inherent and residual risk profile of the relevant obliged entities in a timely fashion.

(13) This Regulation is based on the draft regulatory technical standards submitted by AMLA to the Commission.

HAS ADOPTED THIS REGULATION:

Article 1 – Definitions

1. For the purposes of this Regulation, the following definitions shall apply:

   (a) 'inherent risk' means the risk of money laundering and terrorist financing to which an obliged entity is exposed, because of the products, services and type of transactions it offers, the customers it serves, the jurisdictions in which it operates and the distribution channels it uses to serve its customers, before any mitigating measures have been applied by that obliged entity;

   (b) 'residual risk' means the risk of money laundering and terrorist financing to which an obliged entity remains exposed, after it has put in place policies, procedures, systems and controls to mitigate inherent risk.

Article 2 – Assessment and classification of the inherent risk profile of obliged entities

1. Supervisors shall assess and classify the inherent risk profile of each obliged entity under their supervision that has commenced its activities no later than during the year prior to the year that the assessment and classification takes place.

2. For the purposes of the assessment and classification mentioned in paragraph 1, supervisors shall apply the following sequential steps:

   (a) identify all the inherent risk indicators that apply to the obliged entity and allocate a score to each of these indicators, in accordance with paragraph 3;

   (b) identify all the sub-categories of indicators listed in Section A of Annex I, within the 'products and services' category, that apply to the obliged entity, and calculate a combined score for each of those sub-categories, in accordance with paragraph 4;

   (c) calculate combined scores for all categories of indicators listed in Section A of Annex I, in accordance with paragraph 5;

   (d) calculate the inherent risk score of the obliged entity, in accordance with paragraph 6;

   (e) where the inherent risk score does not adequately reflect the level of ML/TF risks to which the obliged entity is exposed, adjust the inherent risk score, in accordance with paragraph 7;

   (f) classify the inherent risk profile of the obliged entity in accordance with paragraph 8.

3. Each score allocated to an inherent risk indicator shall be a numerical value without decimal places ranging from 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk. The inherent risk indicators shall be established based on the data points listed in Section A of Annex I. The scores shall be calculated based on pre-determined thresholds.

4. A sub-category shall apply only if at least one of its indicators applies to the obliged

entity. Each combined score per sub-category shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk. Each combined score per sub-category shall be calculated from the scores allocated to its inherent risk indicators, in accordance with paragraph 3. For this purpose, supervisors shall use a weighted arithmetic average method. The weight applied to each indicator shall be based on its risk significance. The weights shall be expressed as a numerical value without decimal places ranging from 1, that corresponds to the lowest level of risk significance, to 5, that corresponds to the highest level of risk significance.

5. Each combined score per category shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk. Each combined score per category shall be calculated from the scores allocated to its inherent risk indicators, in accordance with paragraph 3. By way of derogation, the combined score of the 'products and services' category shall be calculated from the combined scores attributed to its sub-categories, in accordance with paragraph 4. For this purpose, supervisors shall use a weighted arithmetic average method. The weight applied to each indicator or sub-category shall be based on its risk significance. The weights shall be expressed as a numerical value without decimal places ranging from 1, that corresponds to the lowest level of risk significance, to 5, that corresponds to the highest level of risk significance.

6. The inherent risk score shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk. The inherent risk score shall be calculated from the combined scores per category determined in accordance with paragraph 5. For this purpose, supervisors shall use a weighted arithmetic average method. The weight applied to each category shall be proportional to the score it received. Categories that received a higher risk score shall have a greater weight than categories that received a lower risk score.

7. The adjustment shall be based on either national specificities or any other circumstances identified by supervisors in the course of their supervisory activities. The adjusted score shall not lead to an increase or decrease by more than one level in accordance with paragraph 8. Where the risk is increased by one level, the adjusted score shall be set at the minimum value of the corresponding level. Where the risk is decreased by one level, the adjusted score shall be set at the maximum value of the corresponding level. The adjustment shall be duly justified and recorded.

8. The classification shall be based on the inherent risk score attributed to the obliged entity in accordance with paragraphs 7 and 8. Supervisors shall classify the inherent risk profile of the obliged entity, in accordance with the following conversion rules:

$$\text{Score} < 1.75\text{: Low risk (1)}$$

$$1.75 \leq \text{Score} < 2.5\text{: Medium risk (2)}$$

$$2.5 \leq \text{Score} < 3.25\text{: Substantial risk (3)}$$

Score ≥ 3.25: High risk (4)

Article 3 – Assessment and classification of the quality of AML/CFT controls put in place by obliged entities

1. Supervisors shall assess and classify the quality of the AML/CFT controls put in place by each obliged entity under their supervision that has commenced its activities no later than during the year prior the year that the assessment and classification takes place.

2. For the purposes of the assessment and classification mentioned in paragraph 1, supervisors shall apply the following sequential steps:

   (a) identify all the controls quality indicators that apply to the obliged entity and allocate a score to each of these indicators, in accordance with paragraph 3;

   (b) calculate combined scores for all applicable categories of indicators listed in Section B of Annex I, in accordance with paragraph 4;

   (c) where supervisors have assessed that a combined score per category does not adequately reflect the level of quality of the controls falling within that category, the score shall be adjusted accordingly, in accordance with paragraph 5;

   (d) calculate the controls quality score of the obliged entity, in accordance with paragraph 6;

   (e) classify the obliged entity in accordance with paragraph 7.

3. Each score allocated to a controls quality indicator shall be a numerical value without decimal places ranging from 1, that corresponds to the highest level of quality, to 4, that corresponds to the lowest level of quality. The controls quality indicators shall be established based on the data points listed in Section B of Annex I. The scores shall be calculated based on pre-determined thresholds.

4. Each combined score per category shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk, to 4 that corresponds to the highest level of risk. Each combined score per category shall be calculated from the scores allocated to its controls quality indicators, in accordance with paragraph 3. For this purpose, supervisors shall use a weighted arithmetic average method. The weight applied to each indicator shall be based on its significance. The weights shall be expressed as a numerical value without decimal places ranging from 1, that corresponds to the lowest level of significance, to 5, that corresponds to the highest level of significance.

5. Each adjustment of a score per category shall be based on a supervisory assessment or an external auditors' assessment available to the relevant supervisor. Each adjustment shall be duly justified and recorded. For the purposes of this paragraph:

   (a) a supervisory assessment shall mean any assessment of the effectiveness, or compliance with AML/CFT legal requirements, of all or part of an obliged entity's AML/CFT governance, procedures, systems and controls carried out by a supervisor within the course of its supervisory activities. This includes,

but is not limited to, full scope or targeted on-site inspections, thematic off-site reviews and other off-site analyses;

(b) an external auditor's assessment shall mean any assessment of the effectiveness, or compliance with AML/CFT requirements, of all or part of an obliged entity's AML/CFT governance, procedures, systems and controls carried out by external auditors.

6. The controls quality score shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk. The controls quality score shall be calculated from the combined scores per category determined in accordance with paragraphs 4 and 5. For this purpose, supervisors shall use a weighted arithmetic average method. The weight applied to each category shall be proportional to the score it received. Categories that received a higher score that corresponds to a lower level of quality shall have a greater weight than categories that received a lower score that corresponds to a higher level of quality.

7. The classification shall be based on the controls quality score attributed to the obliged entity in accordance with paragraph 6. Supervisors shall classify the obliged entity in accordance with the following conversion rules:

$$\text{Score} < 1.75\text{: Very good quality of controls (A)}$$

$$1.75 \leq \text{Score} < 2.5\text{: Good quality of controls (B)}$$

$$2.5 \leq \text{Score} < 3.25\text{: Moderate quality of controls (C)}$$

$$\text{Score} \geq 3.25\text{: Poor quality of controls (D)}$$

Article 4 – Assessment and classification of the residual risk profile of obliged entities

1. Supervisors shall assess and classify the residual risk profile of each obliged entity under their supervision that has commenced its activities no later than during the year prior to the year that the assessment and classification takes place.

2. For the purposes of the assessment and classification mentioned in paragraph 1, supervisors shall apply the following sequential steps:

(a) determine the residual risk score of the obliged entity, based on the inherent risk score and the controls quality score attributed to the obliged entity, in accordance with Article 2 and Article 3;

(b) supervisors shall apply the following rules to combine the inherent risk score and the controls quality score, in accordance with paragraph 1:

(i) where the controls quality score is greater than the inherent risk score, the residual risk score shall be equal to the inherent risk score;

(ii) where the controls quality score is lower than or equal to the inherent risk score, the residual risk score shall be equal to the arithmetic

average of the inherent risk score and the controls quality score;

(c) based on the residual risk score determined in accordance with paragraphs 1 and 2, classify the residual risk profile of the obliged entity, in accordance with the following conversion rules:

Score < 1.75: Low risk (1)

1.75 ≤ Score < 2.5: Medium risk (2)

2.5 ≤ Score < 3.25: Substantial risk (3)

Score ≥ 3.25: High risk (4)

Article 5 – Timelines for and updates to the assessment and classification of the inherent and residual risk profile of obliged entities

1. Supervisors shall carry out the first assessment and classification of the inherent risk and residual risk profiles of obliged entities pursuant to Articles 2, 3 and 4 no later than nine months after the date of application of this Regulation.
2. Supervisors shall carry out any subsequent assessment and classification of the inherent risk and residual risk profile of obliged entities pursuant to Article 2, 3 and 4 by 30 September of the year during which the assessment takes place.
3. By way of derogation from paragraph 2, supervisors shall carry out the assessment and classification of the inherent risk and residual risk profile of an obliged entity pursuant to Article 2, 3 and 4, at least once every three years, where the obliged entity meets any of the following criteria:
   (a) the total number of full-time equivalent employees employed by the obliged entity in the relevant Member State is less than or equal to five;
   (b) the obliged entity carries out only the following activities:
      (i) the activity of an insurance intermediary as referred to in Article 2, paragraph 1, point (6)(c), of Regulation (EU) 2024/1624;
      (ii) the activity of credit intermediary as referred to in Article 2, paragraph 1, point (6)(h), or Article 3, paragraph 3, point (k), of Regulation (EU) 2024/1624;
      (iii) the activity of an insurance undertaking as referred to in Article 2, paragraph 1, point (6)(b), of Regulation (EU) 2024/1624, provided that the obliged entity does not distribute life insurance contracts or products other than: (i) contracts or products that cannot be redeemed; (ii) contracts or products that insure a lender against the death of a borrower; and (iii) contracts or products the annual premium of which does not exceed EUR 1 000 or the corresponding value in the national currency or the unique premium of which does not exceed EUR 2 500 or the corresponding value in the national currency;

(iv) the activity of an investment firm as referred to in Article 2, paragraph 1, point (6)(d), of Regulation (EU) 2024/1624, provided that the obliged entity does not provide (i) any of the investment services listed in points (1), (2), (4), (8) and (9), in Section A of Annex I of Directive (EU) 2014/65, or (ii) any of the ancillary services listed in points (1) and (2), of Section B of Annex I of Directive (EU) 2014/65;

(v) the activity of a creditor as referred to in Article 2, paragraph 1, point (6)(g), of Regulation (EU) 2024/1624;

(vi) the activities listed in points (2), (3) and (6), of Annex I of Directive (EU) 2013/36, with the exception of offering credit agreements relating to immovable property;

(c) the obliged entity is a branch set up by a collective investment undertaking within the meaning of Article 2, paragraph 1, point (6)(e), of Regulation (EU) 2024/1624 in a different Member State; or

(d) the residual risk profile of the obliged entity has already been assessed and classified in accordance with Article 5 at least once, and such residual risk profile was last classified as the low-risk.

4. Where major events or developments in the management and operations of an obliged entity occur, the supervisor shall carry out an ad hoc review of the inherent risk and residual risk profile of the relevant obliged entity. Such assessment and classification shall take place no later than four months after the supervisor become aware of the major event or development.

5. When conducting an ad-hoc assessment pursuant to paragraph 4, the supervisor may decide not to review the scores attributed to indicators that are not affected by the occurrence of the relevant major event or development. The supervisor may also decide not to review the scores of controls categories that are not affected by the occurrence of the relevant major event or development, based on an available supervisory assessment and/or external auditor's assessment.

6. For the purposes of paragraphs 4 and 5, major events or developments in management and operations shall mean any event or development in the management and operations of an obliged entity that may lead to a material change in the obliged entity's inherent risk or residual risk profile. This includes, but is not limited to:

(a) significant changes in the business model of the obliged entity to the extent that these changes may lead to a material change in the obliged entity's inherent risk or residual risk profile;

(b) the identification by the supervisor of significant weaknesses in the entity's AML/CFT procedures, systems and/or controls, to the extent that these weaknesses may lead to a material change in the obliged entity's inherent risk or residual risk profile;

(c) an obliged entity becomes a significant supervised entity within the meaning of Article 2, point (16), of Regulation (EU) 468/2014 or becomes part of a significant supervised group within the meaning of Article 2, point (22), of Regulation (EU) 468/2014, to the extent that this event may lead to a

material change in the obliged entity's inherent or residual risk profile.

Article 6 – Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from [*Date of application*].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President

[For the Commission
On behalf of the President]

[Position]

ANNEX I – Data points, sub-categories and categories

Section A – Inherent risk

[See Annex I, Section A]

Section B – Controls

[See Annex I, Section B]

2.2 Draft RTS on the risk assessment for the purposes of the selection of credit institutions, financial institutions and groups of credit and financial institutions for direct supervision under Article 12(7) of Regulation (EU) 2024/1620

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

supplementing Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 with regard to regulatory technical standards specifying the methodology for assessing credit institutions, financial institutions and groups of credit and financial institutions for the purposes of the selection for direct supervision by the Authority for Anti-Money Laundering and Countering the Financing of Terrorism

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024, establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, and in particular Article 12(7) thereof,

Whereas:

(1) In accordance with Regulation (EU) 2024/1620, certain obliged entities in the financial sector shall be directly supervised by the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (the Authority). The selection of these obliged entities takes place in two stages. In the first stage, the Authority identifies all credit institutions, financial institutions or groups of credit and financial institutions that are operating in at least six Member States, including the home Member State, either via establishment or by conducting relevant operations under the freedom to provide services. In the second stage, the ML/TF risk profile of these entities is classified, to identify those that present a high residual risk.

(2) The ability to provide services in different Member States without having to create an establishment in those Member States is a key feature of the freedom to provide services. In the current context of digitalisation of financial services, a growing number of institutions use this ability to provide their services in other Member States. In some instances, however, entities notify their financial supervisors of their intention

to exercise this freedom but do not start this activity in practice. In other instances, entities exercise this freedom, but it does not represent a major part of their overall operations. Considering the above, materiality thresholds should be established to qualify as eligible for the selection of entities whose operation under the freedom to provide services is material. The thresholds and criteria developed in this Regulation should not be used to define the activity under the freedom to provide services principle for any other purposes.

(3) All entities operating in at least six Member States through establishments or by conducting relevant operations under the freedom to provide services and whose residual risk profile is 'high' should qualify for direct supervision in accordance with Article 13(1) of Regulation (EU) 2024/1620.

(4) To reduce the operational burden on obliged entities and financial supervisors and to ensure alignment between national and EU-level AML/CFT supervision, the assessment of the minimum activities to be carried out by a credit institution or financial institution to be considered as operating in a Member State other than that where it is established, should be based on data points collected for the purpose of the methodology for assessing the risk profiles of obliged entities in line with Article 40(2) of Directive (EU) 2024/1640. For the same reason, the methodology for the selection of directly supervised entities should build on the methodology for assessing the risk profiles of obliged entities in line with Article 40(2) of Directive (EU) 2024/1640. These risk profiles should be aggregated for the classification of the group risk profile, at the level of the highest parent company in the European Union which is a credit or financial institution.

(5) To avoid that, as an effect of the aggregation of the entity-level score, the ML/TF risk profile of a high ML/TF risk group being unduly reduced because some of its components have a low risk profile, the group-wide methodology for the purposes of selection should reflect the relative importance of each entity within the group, in terms of size and risk, and attribute a higher weight to the most important entities.

(6) It is essential to ensure full comparability of the outcomes of the selection process. Given the diversity of approaches adopted by financial supervisors, under the preceding AML/CFT regime which had been established by Directive (EU) 2015/849, to the evaluation of the residual risk profile of obliged entities, the methodology applied for the first round of selection should have different features from the one applied for the subsequent rounds, where a higher degree of harmonisation is envisaged. Some transitional rules should therefore be set, with the objective of limiting the possibility of adjusting the controls quality score based on qualitative assessments of the effectiveness of the entities' controls. This would ensure a smoother transition to the application of the full methodology, when the Authority will have been able to foster, and then ensure, the consistency of supervisory practices.

(7) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the Authority.

HAS ADOPTED THIS REGULATION:

Section 1

Minimum activities to be carried out under the freedom to provide services

Article 1 - Materiality thresholds for operations under the freedom to provide services

1. The minimum activities carried out by a credit institution or a financial institution under the freedom to provide services in a Member State other than the Member State where it is established shall be considered material for the purposes of meeting the conditions of Article 12(1) of Regulation (EU) 2024/1620, where:

   (a) the number of its customers that are resident in that Member State exceeded 20 000 as of 31 December in the previous year; or

   (b) the total annual amount of incoming and outgoing transactions generated by customers referred to in point (a) in the previous year exceeds EUR 50 000 000, or the equivalent in national currency.

2. Whether the activity of the credit or financial institution meets any of the materiality thresholds referred to in paragraph 1, points (a) and (b), shall be determined based on the data points listed in Section C of Annex I.

Section 2

Risk assessment

Article 2 - Assessment and classification of the inherent risk at entity level

1. The methodology for assessing and classifying the inherent and residual risk profile of a credit institution or financial institution as referred to in Article 12, paragraphs (5) and (6), of Regulation (EU) 2024/1640 as low, medium, substantial or high, shall consist of the following sequential steps:

   (a) identify all the inherent risk indicators that apply to the credit institution or financial institution and allocate a score to each of these indicators, in accordance with paragraph 2;

   (b) identify all the sub-categories of indicators listed in Section A of Annex I, within the 'products and services' category, that apply to the credit institution or financial institution, and calculate a combined score for each of those sub-categories, in accordance with paragraph 3;

(c) calculate combined scores for all categories of indicators listed in Section A of Annex I, in accordance with paragraph 4;

(d) calculate the inherent risk score of the credit institution or financial institution, in accordance with paragraph 5;

(e) classify the inherent risk profile of the credit institution or financial institution, in accordance with paragraph 6.

2. Each score allocated to an inherent risk indicator shall be a numerical value without decimal places ranging from 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk. The inherent risk indicators shall be established based on the data points listed in Section A of Annex I. The scores shall be calculated based on pre-determined thresholds.

3. A sub-category shall apply only if at least one of its indicators applies to the credit institution or financial institution. Each combined score per sub-category shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk. Each combined score per sub-category shall be calculated from the scores allocated to its inherent risk indicators, in accordance with paragraph 2. For this purpose, a weighted arithmetic average method shall be used. The weight applied to each indicator shall be based on its risk significance. The weights shall be expressed as a numerical value without decimal places ranging from 1, that corresponds to the lowest level of risk significance, to 5 that corresponds to the highest level of risk significance.

4. Each combined score per category shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk, to 4 that corresponds to the highest level of risk. Each combined score per category shall be calculated from the scores allocated to its inherent risk indicators, in accordance with paragraph 2. By way of derogation, the combined score of the 'products and services' category shall be calculated from the combined scores attributed to its sub-categories, in accordance with paragraph 3. For this purpose, a weighted arithmetic average method shall be used. The weight applied to each indicator or sub-category shall be based on its risk significance. The weights shall be expressed as a numerical value without decimal places ranging from 1, that corresponds to the lowest level of risk significance, to 5, that corresponds to the highest level of risk significance.

5. The inherent risk score shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk. The inherent risk score shall be calculated from the combined scores per category determined in accordance with paragraph 4. For this purpose, a weighted arithmetic average method shall be used. The weight applied to each category shall be proportional to the score it received. Categories that received a higher risk score shall have a greater weight than categories that received a lower risk score.

6. The classification shall be based on the inherent risk score attributed to the credit institution or financial institution in accordance with paragraph 5. The classification shall be made in accordance with the following conversion rules:

Score < 1.75: Low risk (1)

1.75 ≤ Score < 2.5: Medium risk (2)

2.5 ≤ Score < 3.25: Substantial risk (3)

Score ≥ 3.25: High risk (4)

Article 3 - Assessment and classification of the quality of AML/CFT controls

1. The methodology for assessing and qualifying the quality of the AML/CFT controls put in place by a credit institution or financial institution to mitigate the inherent risks to which it is exposed shall consist of the following sequential steps:
   (a) identify all the controls quality indicators that apply to the credit institution or financial institution and allocate a score to each of these indicators, in accordance with paragraph 2;
   (b) calculate combined scores for all applicable categories of indicators listed in Section B of Annex I, in accordance with paragraph 3;
   (c) where supervisors have assessed that a combined score per category does not adequately reflect the level of quality of the controls falling within the relevant category, adjust the score accordingly, in accordance with paragraph 4;
   (d) calculate the controls quality score of the credit institution or financial institution, in accordance with paragraph 5;
   (e) classify the credit institution or financial institution in accordance with paragraph 6.
2. Each score allocated to a controls quality indicator shall be a numerical value without decimal places ranging from 1, that corresponds to the highest level of quality, to 4, that corresponds to the lowest level of quality. The controls quality indicators shall be established based on the data points listed in Section B of Annex I. The scores shall be calculated based on pre-determined thresholds.
3. Each combined score per category shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk. Each combined score per category shall be calculated from the scores allocated to its controls quality indicators, in accordance with paragraph 2. For this purpose, a weighted arithmetic average method shall be used. The weight applied to each indicator shall be based on its significance. The weights shall be expressed as a numerical value without decimal places ranging from 1, that corresponds to the lowest level of significance, to 5, that corresponds to the highest level of significance.
4. Each adjustment of a score per category shall be based on a supervisory assessment or an external auditors' assessment available to the relevant supervisor. Each adjustment shall be duly justified and recorded. For the purposes of this paragraph:
   (a) a supervisory assessment shall mean any assessment of the effectiveness, or compliance with AML/CFT legal requirements, of all or part of a credit institution or financial institution's AML/CFT governance, procedures, systems and controls carried out by a supervisor within the course of its supervisory activities. This includes, but is not limited, to full scope or targeted on-site inspections, thematic off-site reviews and other off-site analyses;

(b) an external auditor's assessment shall mean any assessment of the effectiveness, or compliance with AML/CFT requirements, of all or part of a credit institution or financial institution's AML/CFT governance, procedures, systems and controls carried out by external auditors.

5. The controls quality score shall be a numerical value with two decimal places ranging from 1, that corresponds to the lowest level of risk), to 4, that corresponds to the highest level of risk. The controls quality score shall be calculated from the combined scores per category determined in accordance with paragraphs 3 and 4. For this purpose, a weighted arithmetic average method shall be used. The weight applied to each category shall be proportional to the score it received. Categories that received a higher score that corresponds to a lower level of quality shall have a greater weight than categories that received a lower score that corresponds to a higher level of quality.

6. The classification shall be based on the controls quality score attributed to the credit institution or financial institution in accordance with paragraph 5. The classification shall be made in accordance with the following conversion rules:

$$\text{Score} < 1.75\text{: Very good quality of controls (A)}$$

$$1.75 \leq \text{Score} < 2.5\text{: Good quality of controls (B)}$$

$$2.5 \leq \text{Score} < 3.25\text{: Moderate quality of controls (C)}$$

$$\text{Score} \geq 3.25\text{: Poor quality of controls (D)}$$

Article 4 - Assessment and classification of the residual risk at entity level

The methodology for assessing and classifying the residual risk profile of a credit institution or financial institution, as referred to in Article 12, paragraph (5) and (6), of Regulation (EU) 2024/1640 as low, medium, substantial or high, shall consist of the following sequential steps:

(a) based on the inherent risk score and the controls quality score attributed to the credit or financial institution, in accordance with Article 2 and Article 3, determining the residual risk score of the credit and financial institutions by applying the following rules:

(i) where the controls quality score is greater than the inherent risk score, the residual risk score shall be equal to the inherent risk score;

(ii) where the controls quality score is lower than or equal to the inherent risk score, the residual risk score shall be equal to the average of the inherent risk score and the controls quality score;

(b) depending on the residual risk score of the credit institution or financial institution, determined in accordance with point (a), classifying the residual risk profile of the credit institution or financial institution as low, medium, substantial or high, in accordance with the following conversion rules:

Score < 1.75: Low risk (1)

1.75 ≤ Score < 2.5: Medium risk (2)

2.5 ≤ Score < 3.25: Substantial risk (3)

Score ≥ 3.25: High risk (4)

Article 5 - Group-wide risk assessment

1. The Authority, in collaboration with financial supervisors, shall calculate the group-wide risk profile of a group of credit or financial institutions by aggregating the entity-level residual risk scores of all the credit institutions and financial institutions established in the Union, and which are part of the group.

2. The aggregation referred to in paragraph 1 shall be based on a weighted arithmetic average method, with weights proportional to the relevance of each credit institution or financial institution within the group and enhancing the contribution of riskier entities. For the purpose of the aggregation, the following formula shall be applied:

$$\left(\sum_{i=1}^{N} w[i]r[i]^{\alpha}\right)^{\frac{1}{\alpha}}$$

Where:

N: number of entities in the group

r[i]: residual risk score of entity i

w[i]: weight representing the relevance of entity i within the group

α≥1: parameter to enhance the contribution of risker entities

3. The relevance of each credit institution or financial institution within the group shall be measured in accordance with the data points listed in Section A of Annex I, based on:

   (a) the number of its customers on 31 December of the previous year; and

   (b) the total amount in euro of incoming and outgoing transactions carried out in the previous year or the equivalent in national currency; and

   (c) the total amount in euro of the assets held or managed by the credit institution or financial institution on 31 December of the previous year.

4. The result of the aggregation carried out in accordance paragraph 2 shall be converted into a numerical group-wide residual risk score with two decimal places, ranging between 1, that corresponds to the lowest level of risk, to 4, that corresponds to the highest level of risk.

5. Depending on the residual risk score of the group of credit and financial institutions, its residual risk profile shall be classified as low, medium, substantial or high, in accordance with the following conversion rule:

Score < 1.75: Low risk (1)

1.75 ≤ Score < 2.5: Medium risk (2)

2.5 ≤ Score < 3.25: Substantial risk (3)

Score ≥ 3.25: High risk (4)

Section 3

Final provisions

Article 6 - Transitional provisions

1. The following data points shall not be used for the purposes of the first selection process referred to in Article 13(4) of the Regulation (EU) 2024/1620:
   (a) 'number of customers with high-risk activities' as listed in Section A of Annex I;
   (b) 'number of customers whose CDD data and information is not yet in line with the requirements of Article 20 AMLR' as listed in Section B of Annex I.
2. Article 3, paragraph 1, point (c), shall not apply to the assessment of the quality of controls performed for the purposes of the first selection process referred to in Article 13(4) of Regulation (EU) 2024/1620.
3. By way of derogation from paragraph 2, the controls quality score may be adjusted by increasing or decreasing it by one level, based on outcomes of on-site inspections that took place in the two calendar years before the launch of the assessments, where this information is relevant for the classification of the entity's ML/TF risk profile. Where the risk is increased by one level, the adjusted score shall be set at the minimum value of the corresponding level. Where the risk is decreased by one level, the adjusted score shall be set at the maximum value of that corresponding level.
4. The adjustment applied in accordance with paragraph 3 shall always be duly justified and recorded.

Article 7 - Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from [*Date of application*].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President

[For the Commission
On behalf of the President]

[Position]

2.3 Draft RTS on Customer Due Diligence under Article 28(1) of Regulation (EU) 2024/1624

COMMISSION DELEGATED REGULATION (EU) …/...

of XXX

on supplementing Regulation (EU) 2024/1624 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information and requirements necessary for the performance of customer due diligence for the purposes of Article 28(1)

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and in particular Article 28(1), points (a) to (e) thereof,

Whereas:

(1) Regulation (EU) 2024/1624 aims for harmonisation of customer due diligence measures across Member States and obliged entities within the EU. To achieve this, this Commission Delegated Regulation ('Regulation') sets common parameters for the application of customer due diligence measures. Obliged entities are required to adjust the customer due diligence measures based on the ML/TF risk associated with their customers, business relationships or an occasional transaction. This will ensure a proportionate and effective approach. Accordingly, obliged entities shall collect the information on a risk-sensitive basis and apply the measures laid down in this Regulation, ensuring that their scope, intensity and frequency are proportionate to the customer's money laundering and terrorist financing risk profile.

(2) Obliged entities should, when identifying a customer and verifying their identity, collect data and information in a consistent way in all Member States. The same approach should apply to all customers, whether they are a natural person or a legal person.

(3) Obliged entities should collect information to understand the nationality and the place of birth of customers who are natural persons. Since not all government-issued identity documents contain information on the holder's nationality or their place of birth, obliged entities may need to obtain that information from other sources. Where a person holds multiple nationalities and declares them in good faith, verifying one nationality will be sufficient. In situations where the person is stateless, or has refugee or subsidiary protection status, this information should instead be obtained.

(4) Information collected by obliged entities for customer due diligence purposes may not always be in the form of documents. This Regulation specifies the situations where documents should be collected.

(5) Obtaining data and documents from independent and reliable sources is key to ensuring that obliged entities can be satisfied that they know who their customers are. Reliable and independent sources of information for customers that are not natural persons include, but are not limited to: statutory documents of the legal entity or legal arrangement required by law, including certificates of incorporation or audited financial statements; the most recent version of the constitutive documents establishing the legal entity or legal arrangement, including the Memorandum of Association and Articles of Association, or a recent official copy of these documents issued by the applicable public registers and lists or an unofficial copy thereof certified by an independent professional or a public authority. In the case of a trust or similar legal arrangement that may not be subject to registration, a recent copy of the trust deed, or an extract thereof, together with any other document that determines the exercise of any powers by the trustees or similar administrators, certified by an independent professional, could qualify as reliable and independent sources of information.

(6) Obliged entities should assess the level of reliability and independence of the sources of information they have obtained as part of their customer due diligence process based on certain criteria. For example, unless it has been issued by a state or public authority, a recent document may be more reliable than information that dates back several years. Once such assessment of a certain source is completed, the results of such assessment can be used for multiple customers.

(7) There may be situations where identity documents issued to or held by the customer do not meet the attributes of an identity card or passport. This could be the case, for example, where the customer has credible and legitimate reasons for being unable to provide traditional forms of identity documentation: being an asylum seeker; a refugee; a person to whom a residence permit was not granted, but whose repatriation is impossible for legal or factual reasons; being homeless or being otherwise vulnerable. Regulation (EU) 2024/1624 does not provide an exemption from the list of information obliged entities should collect for natural persons in this category. To mitigate the risk of financial exclusion and unwarranted de-risking, this Regulation makes the approach more flexible by allowing obliged entities to obtain the requested information from these natural persons via other credible means.

(8) Obtaining beneficial owner information for all customers that are not natural persons is essential for complying with anti-money laundering and countering the financing of terrorism (AML/CFT) requirements and with targeted financial sanctions obligations. For this reason, consultation of central registers for information on beneficial owners is necessary but not sufficient to fulfil the verification requirements.

(9) There are legitimate situations where the obliged entity may be unable to identify a natural person as the beneficial owner of its customer. In these situations, Regulation (EU) 2024/1624 instead requires the identification of senior managing officials (SMOs). While SMOs are not beneficial owners, for the purposes of identification and verification measures, obliged entities should collect equivalent information for SMOs as they do for the beneficial owners.

(10) The identification of SMOs is permitted under Regulation (EU) 2024/1624 only in cases where the obliged entity has been unable to identify beneficial owners having

'exhausted all possible means of identification' or where 'there are doubts that the persons identified are the beneficial owners'. Finding it difficult to identify the beneficial owner, for example in cases of complex corporate structures, does not amount to 'doubts' and therefore will not provide a sufficient basis for the obliged entity to instead identify the SMOs.

(11) When collecting information on the identity of SMOs for the purposes of Article 63(4), point (b), of Regulation (EU) 2024/1624, the obliged entity may collect the address of the registered office of the legal entity instead of the residential address and country of residence required under Article 62(1), second subparagraph, point (a), of Regulation (EU) 2024/1624.

(12) Understanding the purpose and intended nature of a business relationship or occasional transaction is an important component of the customer due diligence process and the modalities are set out in Article 25 of Regulation (EU) 2024/1624. Obliged entities should assess whether the information already at their disposal is sufficient to understand its purpose and intended nature. In situations where they need further information in order to be satisfied that they understand the purpose and intended nature of the business relationship or occasional transaction, this Regulation specifies which information obliged entities should obtain before entering into a business relationship or performing an occasional transaction to satisfy their information needs.

(13) Article 20(1), point (h), of Regulation (EU) 2024/1624 requires that obliged entities identify and verify the identity of the natural person on whose behalf or for the benefit of whom a transaction or activity is being conducted. This Regulation lays down specific rules for the identification and verification of the identity of the final investors of a collective investment undertaking (CIU) that distributes its shares or units through another credit or financial institution, which acts in its own name but on behalf or for the benefit of one or more final investors. To ensure the effectiveness of customer due diligence measures and the proportionality of their application, it is appropriate to allow CIUs, where the relationship with the intermediary institution is assessed as low or standard risk, to rely on that institution for the identification and verification of the final investors, provided that strict conditions are met and that information on the final investors can be obtained without undue delay.

(14) Regulation (EU) 2024/1624 requires specific measures to be applied to transactions or business relationships with politically exposed persons (PEPs). The focus of this Regulation is on measures for the identification, by obliged entities, of politically exposed persons, their family members or persons known to be close associates. PEP screening measures should apply to the customer, its beneficial owner and the person on whose behalf or for the benefit of whom a transaction or activity is being carried out. These measures are important because once a PEP is identified, the obliged entity should apply specific and additional customer due diligence measures in relation to that customer.

(15) In situations where the ML/TF risk is assessed as low, Regulation (EU) 2024/1624 allows the application of simplified due diligence measures. Simplified due diligence measures should ease the administrative burden on obliged entities and on their customers.

(16) Minimum requirements for the identification of natural persons in low-risk situations should include at least the type of information that is usually included in a passport or identity document. This ensures that obliged entities have sufficient and verifiable information to establish the identity of their customers, while keeping the requirements proportionate to the lower level of ML/TF risk.

(17) This Regulation identifies a service that would benefit from specific simplified due diligence measures. This is the case where a credit institution opens a pooled account for a customer that is an obliged entity, to hold or administer funds that belong to the customer's own clients, where the ML/TF risk of that service is assessed as low, based on the credit institution's risk assessment. In such cases, since the final customers are already subject to the customer due diligence measures applied by the obliged entity, it is proportionate to allow specific simplified due diligence measures, in order to avoid duplication of controls while ensuring that appropriate safeguards remain in place. Situations where credit institutions open a payment account for payment institutions or electronic money institutions will fall outside the scope of the sectoral simplified measures provision of this Regulation. Such situations would be regarded as correspondent relationships within the meaning of Article 2(22), point (b), of Regulation (EU) 2024/1624.

(18) In situations where the ML/TF risks are higher, Regulation (EU) 2024/1624 calls for the application of enhanced due diligence measures to manage and mitigate these risks appropriately. Where obliged entities obtain additional information in relation to the measures mentioned in Article 34(4) of Regulation (EU) 2024/1624 to meet these requirements and to mitigate the higher risk appropriately and effectively, this information should be of sufficient quality to enable them to assess the authenticity and accuracy of the information provided. It should also meet the criteria of reliability and independence.

(19) Additional information obliged entities obtain for understanding the source of funds and the source of wealth of the customer and of the beneficial owners in high-risk situations should enable them to satisfy themselves that the funds and assets used by the customer and beneficial owners are of legitimate origin.

(20) Customer due diligence measures include a specific requirement for obliged entities to verify whether the customer or the beneficial owner is subject to targeted financial sanctions as defined by Article 2(49) of Regulation (EU) 2024/1624. Screening for the application of trade or economic sanctions such as arms embargoes, trade restrictions or travel bans falls outside the scope of Regulation (EU) 2024/1624 and, consequently, of this Regulation.

(21) Article 19(7) of Regulation (EU) 2024/1624 provides for a list of four conditions on the basis of which AML/CFT supervisors may decide to grant an exemption for electronic money issuers from the customer due diligence measures in Article 20(1), points (a), (b) and (c), of that Regulation. To enable supervisors to determine the extent of such exemption (i.e. 'fully or partially') in a consistent way across Member States, this Regulation provides AML/CFT supervisors with a non-exhaustive list of risk factors associated with features of electronic money instruments.

(22) The use of attributes of means of electronic identification and qualified trust services for customer due diligence purposes should be aligned with the risk of ML/TF posed by the customer or beneficial owner.

(23) Obliged entities need to ensure that their customer information remains up to date. The maximum periods of 1 and 5 years, respectively, for updating customer information in accordance with the requirements of the Regulation (EU) 2024/1624 should only start with the application date of this Commission Delegated Regulation for existing customers onboarded before Regulation (EU) 2024/1624 took effect.

HAS ADOPTED THIS REGULATION:

Section 1

General principles

Article 1 - Proportionality and risk-based approach

This Commission Delegated Regulation ('Regulation') shall be applied in line with the risk-based approach. The extent and the nature of the information to be obtained and the measures to be applied by obliged entities shall be commensurate with the type and level of risk identified and shall enable obliged entities to manage and mitigate that risk appropriately.

Section 2

Information to be collected for identification and verification purposes

Article 2 - Information to be obtained in relation to names

1. In relation to the names and surnames of a natural person as referred to in Article 22(1), point (a)(i), of Regulation (EU) 2024/1624, obliged entities shall obtain all names and surnames that feature on the identity document, passport or equivalent.
2. In relation to the name of a legal entity as referred to in Article 22(1), point (b)(i), and other organisations that have legal capacity under national law as referred to in Article 22(1), point (d)(i), of Regulation (EU) 2024/1624, obliged entities shall obtain the registered name and the trade name where it differs from the registered name.

Article 3 - Information to be obtained in relation to addresses

The information on the address as referred to in provisions of Article 22(1) of Regulation (EU) 2024/1624 shall consist of the following information:

(a) the full country name or the abbreviation in accordance with the International Standard for country codes (ISO 3166);

(b) the city, or its nearest alternative;

(c) where available, postal code, street name, post boxes, building number and the apartment number.

Article 4 - Specification on the provision of the place of birth

The information on place of birth as referred to in Article 22(1), point (a)(ii), of Regulation (EU) 2024/1624 shall consist of at least the country name. Should the identity document, passport or equivalent of the customer provide additional information on place of birth, such information shall be collected.

Article 5 - Specification on nationalities

For the purposes of Article 22 (1), point (a)(iii), of Regulation (EU) 2024/1624 obliged entities shall obtain information on all nationalities or, where applicable, the statelessness and refugee or subsidiary protection status of the customer, any natural person purporting to act on behalf of the customer, and the natural persons on whose behalf or for the benefit of whom a transaction or activity is being conducted.

Article 6 - Documents for the verification of identity

1. For the purposes of verifying the identity of the natural person in accordance with Article 22(6), point (a), and Article 22(7), point (a), of Regulation (EU) 2024/1624, a document shall be considered equivalent to an identity document or passport if it meets all of the following conditions:
   (a) it is issued by a state or public authority;
   (b) it contains all names and surnames and the holder's date of birth;
   (c) it contains information on the date of expiration and a document number;
   (d) it contains a facial image and the signature of the document holder;
   (e) it contains security features to ensure authenticity.
2. In situations where the natural person cannot provide an identity document, passport or a document that meets the requirements in paragraph 1 for a legitimate reason such as their statelessness or refugee or subsidiary protection status, a document shall be considered equivalent to an identity document or passport if it meets all of the following requirements:
   (a) it is issued by a state or public authority;
   (b) it contains all names and surnames of the natural person;
   (c) it contains the date of birth of the natural person;
   (d) it contains a facial image of the document holder.

   If the document provided does not include information stipulated in the points of the first subparagraph, obliged entities shall use other credible means to obtain this information.
3. Obliged entities shall take reasonable steps to ensure that all documents obtained for the verification of the identity of the natural person pursuant to Article 22(6), point (a)

and Article 22(7), point (a), of Regulation (EU) 2024/1624, as referred to in paragraphs 1 and 2, are authentic and have not been forged or tampered with.

4. When original documents are in a foreign language, obliged entities shall ensure that they understand their content.

5. For the purposes of verifying the identity of the persons referred to in Article 22(6) and Article 22(7), point (a), of Regulation (EU) 2024/1624, obliged entities shall obtain from that person the identity document, passport or equivalent, or a certified copy thereof, or in accordance with Article 7.

6. Electronic identification means, as described in Article 7(1), shall be permitted to verify the identity of the natural person in a face-to-face context where they are available to the customer, any person purporting to act on behalf of the customer, and the natural persons on whose behalf or for the benefit of whom a transaction or activity is being carried out.

Article 7 - Verification measures conducted on a non-face-to-face basis

1. To comply with the verification requirements pursuant to Article 22(6) of Regulation (EU) 2024/1624 in a non-face-to-face situation, obliged entities shall use electronic identification means that meet the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels 'substantial' or 'high', or relevant qualified trust services as set out in that Regulation.

2. In cases where the solution described in paragraph 1 is not available, or cannot reasonably be expected to be provided, obliged entities shall obtain the natural person's identity document, passport or equivalent using remote solutions that meet the conditions set out in paragraphs 3-5.

3. Obliged entities shall ensure that the solution described in paragraph 2 uses reliable and independent information sources and includes the following safeguards regarding the quality and accuracy of the data and documents to be collected:

   (a) controls to ensure that the natural person presenting the customer's identity document, passport or equivalent is the person on the picture of the document;

   (b) the integrity and confidentiality of the communication are ensured;

   (c) any images, video, sound and/or data are captured in a readable format and with sufficient quality so that the natural person is unambiguously recognisable;

   (d) where applicable, the identification process does not continue if technical shortcomings or unexpected connection interruptions are detected or there are any doubts regarding the identity of the natural person;

   (e) the information obtained through the remote solution is up-to-date;

   (f) the documents and information collected during the remote verification process, which are required to be retained, are time-stamped and stored securely by the obliged entity. The content of stored records, including images, videos, sound and data shall be available in a readable format and allow for *ex-post* verifications.

4. Where obliged entities accept reproductions of an original document for customers that are not natural persons and do not examine the original document, obliged entities shall take reasonable steps to ascertain that the reproduction is reliable.
5. Obliged entities using remote solutions shall be able to demonstrate to their competent authority that the remote verification solutions they use comply with the provisions included in this Article and that they meet the requirements stipulated by the applicable data protection legislation.

Article 8 - Reliable and independent sources of information

In order to determine whether a source of information is reliable and independent, obliged entities shall take risk-sensitive measures to assess:

(a) the credibility of the source, including its reputation;

(b) the official status and independence of the information source;

(c) the extent to which the information is up-to-date;

(d) the accuracy of the source, based on whether the information or data provided had to undergo certain checks before being provided or is consistent with other sources;

(e) the ease with which the identity information or data provided can be forged.

Article 9 - Identification and verification of the identity of the natural or legal persons using a virtual IBAN

For the purposes of Article 22(3) of Regulation (EU) 2024/1624, the information to be obtained to identify and verify the identity of the natural or legal persons using the virtual IBAN shall include:

(a) the information required pursuant to Article 22(1) of Regulation (EU) 2024/1624;

(b) the virtual IBAN number assigned to that natural person or legal person;

(c) the dates on which the associated bank or payment account was opened and, where applicable, closed.

Article 10 - Reasonable measures for verification of the beneficial owner

The reasonable measures referred to in Article 22(7), point (b), of Regulation (EU) 2024/1624 shall include at least one of the following:

(a) consulting public registers, other than the central registers, or other reliable national systems that contain the information necessary to verify the identity of the beneficial owner, or the person on whose behalf or for the benefit of whom the transaction or activity is being carried out, such as the residence register, tax register, passport database and the land register, to the extent that these are accessible to obliged entities; or

(b) collecting information from the customer or other sources, which may include third-party sources such as:

i. reputable credit agencies and/or comparable reputable data services providers;
ii. utility bills;
iii. up-to-date information from credit or financial institutions as defined in Article 3, paragraphs (1) and (2), of Regulation (EU) 2024/1624. The collected information shall confirm that the beneficial owner or the person on whose behalf or for the benefit of whom a transaction or activity is being carried out has been identified and verified by the respective institution;
iv. documents from the legal entity or the legal arrangement where the beneficial owner is named, and where the identity of the named person is certified by persons that are authorised for document certification purposes.

Article 11 - Understanding the ownership and control structure of the customer

1. For the purposes of understanding the ownership and control structure of the customer in accordance with Article 20(1), point (b), of Regulation (EU) 2024/1624 and in situations where the customer's ownership and control structure contains more than one legal entity or legal arrangement, obliged entities shall take risk-sensitive measures to obtain the following information:

   (a) a description of the ownership and control structure, including the legal entities and/or legal arrangements that constitute intermediate entities between the customer and their beneficial owners and relevant for understanding the ownership and control structure; and

   (b) where applicable:

      i. where beneficial ownership is determined on the basis of control, information on how this is expressed and exercised; or

      ii. information on the regulated market on which the securities are listed, in case a legal entity at an intermediate level of the ownership and control structure has its securities listed on a regulated market, and the number and percentage of shares listed if not all the legal entity's securities are listed on a regulated market.

2. With respect to the legal entities and/or legal arrangements described in paragraph (1), point (a), and to the extent that it is relevant, obliged entities shall take risk-sensitive measures to obtain the following information:

   (a) the legal form of such entities and/or arrangements, and reference to the existence of any nominee shareholders;

   (b) the jurisdiction of incorporation or registration of the legal person or legal arrangement,

   (c) in the case of a trust, the jurisdiction of its governing law;

   (d) where applicable, the shares of interest held by each legal entity or legal arrangement, its sub-division, by class or type of shares and/or voting rights expressed as a percentage of the respective total.

3. When obliged entities assess the ownership and control structure, they must be satisfied that:

   (a) the information included in the description is credible;

(b) that there is an economic rationale behind the structure; and

(c) that they understand how the overall structure affects the ML/TF risk associated with the customer.

Article 12 - Understanding the ownership and control structure of the customer in the case of complex corporate structures

1. To understand the ownership and control structure of the customer in accordance with Article 20(1), point (b), of Regulation (EU) 2024/1624, obliged entities shall treat an ownership and control structure as a complex corporate structure where there are three or more layers between the customer and the beneficial owner and, in addition, more than one of the following conditions is met:

   (a) there is a legal arrangement or a similar legal entity such as a foundation in any of the layers;

   (b) the customer and any legal entities present at any of these layers are registered in jurisdictions outside the EU;

   (c) there are nominee shareholders or nominee directors involved in the structure;

   (d) the structure obfuscates or diminishes transparency of ownership with no legitimate economic rationale or justification.

2. When some of the conditions stipulated in paragraph 1 are met, obliged entities shall take reasonable measures, and where necessary, obtain additional information, such as an organigram, needed to complement the information collected under Article 11(1), to understand the complex corporate structure.

3. Obliged entities shall take risk-sensitive measures to satisfy themselves that the information obtained is accurate and provides obliged entities with a comprehensive understanding of the ownership and control structure of the customer.

Article 13 - Information on senior managing officials

In relation to senior managing officials as referred to in Article 22(2), second subparagraph, of Regulation (EU) 2024/1624, obliged entities shall:

(a) collect the same information as the information they would collect for beneficial owners. Obliged entities may decide to obtain the address of the registered office of the legal entity instead of the senior managing official's residential address and country of residence;

(b) verify the identity of senior managing officials in the same way as they would for beneficial owners.

Article 14 - Identification and verification of beneficiaries of trusts and similar legal entities or arrangements

1. For the purposes of Article 22(4) of Regulation (EU) 2024/1624, the information obliged entities shall obtain from the trustee, legal entity or legal arrangement include:

(a) a description of the class of beneficiaries and its characteristics, which shall contain sufficient information to allow the obliged entity to determine whether individual beneficiaries are ascertainable and shall be treated as beneficial owners; and

(b) relevant documents to enable the obliged entity to establish that the description is correct and up-to-date.

2. Obliged entities shall take risk-sensitive measures to ensure that the trustee, legal entity or legal arrangement provide timely updates, including on specific material events that may lead to beneficiaries previously identified by class or characteristics becoming ascertainable and thus beneficial owners.

Article 15 - Identification and verification of beneficiaries of discretionary trusts

1. For the purposes of Article 22(5) of Regulation (EU) 2024/1624, the information obliged entities shall obtain from the trustee of the discretionary trust include:

(a) details on the objects of a power and default takers, to establish whether it is a class of natural or legal persons or if the natural or legal persons are already identified;

(b) relevant documents to enable the obliged entity to establish that these details are correct and up-to-date.

2. To comply with paragraph 1, obliged entities shall take risk-sensitive measures to:

(a) obtain sufficient information about how and in which ways the power of discretion can be exercised by the trustee(s);

(b) establish whether trustees have exercised their power of discretion and appointed one or more beneficiaries from among the objects of a power, or whether the default takers have become the beneficiaries due to the trustees' failure to exercise their power of discretion.

Article 16 - Identification and verification of the person purporting to act on behalf of the customer

In relation to the identification and verification of the person purporting to act on behalf of the customer as referred in Article 22 of Regulation (EU) 2024/1624, and in addition to the information to be collected pursuant to the relevant provisions of Section 2, obliged entities shall obtain information which enables them to verify the existence and extent of the power of representation.

Article 17 - Identification and verification obligations for collective investment undertakings

When a collective investment undertaking distributes its shares or units through another credit institution or financial institution that acts in its own name but on behalf or for the benefit of one or more final investors, it may fulfil the requirement under Article 20(1), point (h), of Regulation (EU) 2024/1624 if it is satisfied that the credit institution or financial

institution will provide the information necessary to identify and verify the identity of the final investors without undue delay and upon request. This applies provided that:

(a) the credit institution or financial institution is subject to AML/CFT obligations in an EU Member State or in a third country that has AML/CFT requirements that are no less robust than those stipulated by Regulation (EU) 2024/1624;

(b) the credit institution or financial institution is effectively supervised for compliance with obligations as provided for in point (a);

(c) the risk associated with the relationship with the credit or financial institution is low or standard; and

(d) the collective investment undertaking is satisfied that the credit institution or financial institution applies robust and risk-sensitive CDD measures to its own customers and its customers' beneficial owners.

Section 3

Purpose and intended nature of the business relationship or the occasional transaction

Article 18 - Identification of the purpose and intended nature of a business relationship or occasional transaction

For the purposes of Article 20(1), point (c), and Article 25 of Regulation (EU) 2024/1624, obliged entities shall obtain, where necessary:

(a) in relation to the purpose and economic rationale of the occasional transaction or business relationship, taking into account the nature of the product or service provided, at least one of the following information:

  i. the reason the customer has requested the obliged entities' products or services;

  ii. the intended use of the products or services requested by the customer;

  iii. the reason for performing the occasional transaction;

  iv. whether the customer has additional business relationships with the obliged entity or, where applicable, its wider group, and the extent to which that influences the obliged entity's understanding of the customer.

(b) in relation to the estimated amount of the envisaged activities, at least one of the following information:

  i. the estimated amount of funds to be deposited;

  ii. information to understand the anticipated number, size, volume, type and frequency of transactions that are likely to be performed during the business relationship or occasional transaction.

(c) in relation to the source of funds, at least one of the following information to understand the activity that generated the funds and the means through which the customer's funds were transferred:

i. employment income, including salary, wages, bonusses and other compensation from employment;

ii. pension or retirement funds and government benefits including social benefits;

iii. grants;

iv. business revenue;

v. capital provided by shareholders and intercompany funding;

vi. loans and credit facilities;

vii. savings and investments income;

viii. inheritance, gifts, sales of assets and legal settlements.

(d) in relation to the destination of funds, at least one of the following information:

i. the expected types of recipient(s);

ii. the jurisdiction where the transactions are to be received;

iii. whether the recipient of funds is the intended beneficiary of the transferred funds, or acting as intermediary for the beneficiary.

(e) in relation to the business activity or the occupation of the customer, at least one of the following information:

i. the occupation of the customer, including information on the customer's employment status;

ii. the sector in which the customer is active, including information on customer's industry, operations, products and services;

iii. whether the business activity or the occupation of the customer is regulated;

iv. whether the customer is an obliged entity and the sector in which the customer operates;

v. whether the customer is actively engaged in business;

vi. geographical presence of the customer;

vii. information on the main sources of revenues of the customer;

viii. key stakeholders of the customer.

Section 4

Politically Exposed Persons

Article 19 - Identification of Politically Exposed Persons

1. To identify a politically exposed person or a family member[6], or person known to be a close associate[7] of a politically exposed person, pursuant to Article 20(1), point (g), of Regulation (EU) 2024/1624, obliged entities shall determine:

   (a) before the establishment of the business relationship or the carrying out of the occasional transaction, if the customer, the beneficial owner of the customer and, where relevant, the person on whose behalf or for the benefit of whom a transaction or activity is being carried out, is a politically exposed person, a family member, or person known to be a close associate; and

   (b) whether existing customers, the beneficial owner of the customer and, where relevant, the person on whose behalf or for the benefit of whom a transaction or activity is being carried out have become politically exposed persons, family members or persons known to be a close associate.

2. Obliged entities shall perform a review of whether the persons specified in paragraph 1, point (b), qualify as politically exposed persons:

   (a) with a frequency established on the basis of a risk-sensitive approach;

   (b) without delay in case of new information or changes in information collected for the purposes of the performance of customer due diligence measures that may have an impact on identification as a politically exposed person,

   (c) the beneficial owner of the customer and, where relevant, the person on whose behalf or for the benefit of whom a transaction or activity is being carried out, has become a:
      i. politically exposed person;
      ii. family member of a politically exposed person; or
      iii. person known to be a close associate of a politically exposed person;

   (d) without delay in case of changes and amendments to the list of prominent public functions published pursuant to Article 43(5) of the Regulation (EU) 2024/1624.

3. To comply with paragraphs 1 and 2, obliged entities shall put in place automated screening tools and measures, or a combination of automated screening tools and manual checks unless the size, business model, complexity or nature of the business of the obliged entity justifies the use of manual checks only.

Section 5

Simplified Due Diligence measures

Article 20 - Minimum requirement for customer identification in situations of low risk

1. In situations of low risk, obliged entities shall obtain at least the following information to identify the customer and the person purporting to act on behalf of the customer:

   (a) for a natural person:

[6] Article 2(1), point (35) of Regulation (EU) 2024/1624.

[7] Article 2(1), point (36) of Regulation (EU) 2024/1624.

i. all names and surnames;

ii. place of birth;

iii. date of birth;

iv nationalities of the natural person or their statelessness, refugee or subsidiary protection status.

(b) for a legal entity and other organisations that have legal capacity under national law:

i. the legal form;

ii. the registered name of the legal entity and its trade name where it differs from its registered name;

iii. the address of the registered office; and

iv. where available, the registration number or tax identification number, or the legal entity identifier.

2. Paragraph 1 shall also apply to persons on whose behalf or for the benefit of whom a transaction or activity is being carried out.

Article 21 - Minimum requirements for the identification and verification of beneficial owner or senior managing officials in situations of low risk

1. To identify the beneficial owner or senior managing officials in situations of low risk, obliged entities shall consult one of the following sources of information:

(a) the information contained in the central register, business or company register;

(b) any information provided by the customer, including information that obliged entities may already hold;

(c) any publicly available information contained in a reliable independent open source.

2. To verify the identity of the beneficial owner or senior managing officials in situations of low risk, the obliged entity shall consult one of the sources of information listed in paragraph (1), points (b) or (c), that was not used for identification purposes.

Article 22 - Sectoral simplified measures with respect to pooled accounts

A credit institution that opens an account in which the account holder administers the funds of its clients fulfils the requirements stipulated in Article 20(1), point (h), of Regulation (EU) 2024/1624, if all of the following conditions are met:

(a) the credit institution is satisfied that the account holder will provide customer due diligence information and documents related to clients for whom it administers their funds, immediately after such request has been made by the credit institution;

(b) the account holder is an obliged entity that is subject to AML/CFT obligations in an EU Member State or a third country with AML/CFT requirements that are no less robust than those stipulated by Regulation (EU) 2024/1624;

(c) the account holder is effectively supervised for compliance with obligations as provided for in point (b);

(d) the ML/TF risk associated with the business relationship is low;

(e) the credit institution is satisfied that the account holder applies robust and risk-sensitive customer due diligence measures on its clients and the clients' beneficial owners.

Article 23 - Customer identification data updates in low-risk situations

1. Where, in cases with a low degree of ML/TF risk, obliged entities reduce the frequency of customer identification updates as referred to in Article 33(1), point (b), of Regulation (EU) 2024/1624, obliged entities shall monitor the relationship in order to be satisfied that:

   (a) there is no change in the circumstances relevant for the assessment of the business relationship with the customer;

   (b) no event took place which would require an information update; and

   (c) no suspicious and/or unusual transactions or activities were identified that are inconsistent with a low-risk relationship.

2. In any case, obliged entities shall update the customer identification data in accordance with Article 26(2), point (b), of Regulation (EU) 2024/1624.

Article 24 - Minimum information to identify the purpose and intended nature of the business relationship or occasional transaction in low-risk situations

In order to apply simplified due diligence measures pursuant to Article 33(1), point (c), of Regulation (EU) 2024/1624, obliged entities shall at least take risk-sensitive measures to understand:

(a) the intended use of the products or services requested by the customer;

(b) where applicable, the estimated value of transactions during the business relationship or of the occasional transaction;

(c) where necessary, the source of funds.

Section 6

Enhanced Due Diligence measures

Article 25 - Additional information on the customer and the beneficial owners

For the purposes of Article 34(4), point (a), of Regulation (EU) 2024/1624, obliged entities shall obtain one or more of the following additional information that will allow them to:

(a) be satisfied that the information they hold on the customer and the beneficial owners or the ownership and control structure of the customer other than a natural person is authentic and accurate; or

(b) assess the reputation of the customer and the beneficial owners; or

(c) identify and assess in a comprehensive way ML/TF risks associated with the customer, the beneficial owners or any close relationships known to the obliged entity or that are publicly known.

Article 26 - Additional information on the intended nature of the business relationship

1. For the purposes of Article 34(4), point (b), of Regulation (EU) 2024/1624, obliged entities shall obtain one or more of the following additional information on the intended nature of the business relationship that will allow them to:

   (a) be satisfied that the information they hold is authentic and accurate when it comes to information on the intended nature of the business relationship; or

   (b) be satisfied that the destination of funds is consistent with the stated nature of the business relationship or occasional transaction and the customer's risk profile; or

   (c) assess that the expected number, size, type, volume and frequency of transactions that are expected to be performed are consistent with the declared business activity, source of funds or source of wealth of the customer.

2. For the purposes of points (a) to (c) of paragraph 1, information to be obtained by obliged entities may consist of additional information on the customer's key customers, contracts, business partners, associates or the occasional transaction, including, where relevant, the beneficial owner's business partners or associates.

Article 27 - Additional information on the source of funds, and source of wealth of the customer and of the beneficial owners

For the purposes of Article 34(4), point (c), of Regulation (EU) 2024/1624, obliged entities shall obtain such additional information on the source of funds, and source of wealth of the customer and of the beneficial owners, that will satisfy them that the source of funds or source of wealth is derived from lawful activities. Such information may include one or more of the following:

(a) in relation to proof of income:

   i. tax declarations;

   ii. recent pay slips or employment documentation specifying at least the amount of salary;

   iii. other official income statements;

(b) audited accounts, investment documentation, credit facility agreements and loan agreements;

(c) in case of immovable property, public deeds, or abstract from the land or residents registry;

(d) inheritance, gifts and legal settlements documentation, documentation from certified independent professionals or public authorities;

(e) contract of sale or written confirmation of sale;

(f) information from reliable asset or public registers;

(g) authentic information from reputable media publications or reputable commercially available service providers;

(h) any other relevant information from independent and reliable sources, providing a high degree of reassurance that the customer's and beneficial owners' source of funds, and source of wealth are not the proceeds of criminal activity and are consistent with the obliged entities' knowledge of the customer and the nature of the business relationship.

Article 28 - Information on the reasons for the intended or performed transactions and their consistency with the business relationship

For the purposes of Article 34(4), point (d), of Regulation (EU) 2024/1624, obliged entities shall obtain one or more of the following information on the reasons for the intended or performed transactions and their consistency with the business relationship, on which basis they can assess:

(a) the extent to which the reason provided for the transaction is credible and in line with the institution's knowledge of the customer; or

(b) the consistency of the overall transactions performed during the business relationship with the activities carried out and the customer's turnover, especially in the case of economic activities characterised by the use of assets representing higher ML/TF risks; or

(c) information to clarify any higher risks the obliged entity may have identified in respect of the parties involved in the transaction, including any intermediaries, and their relationship with the customer.

Section 7

Targeted Financial Sanctions

Article 29 - Screening of customers and beneficial owners

Obliged entities shall establish whether their customers, the beneficial owners and the entities or persons which control or meet the ownership conditions stipulated in Article 20(1), point (d), of Regulation (EU) 2024/1624 are subject to targeted financial sanctions. Where there is a suspicion of circumvention or evasion of targeted financial sanctions, obliged entities shall also establish whether the person acting on behalf of the customer is subject to targeted financial sanctions.

Article 30 - Screening requirements

For the purposes of Article 29, obliged entities shall:

(a) screen, through automated screening tools or solutions, or a combination of automated screening tools and manual checks, at least the following information on customers,

beneficial owners and the entities or persons which control or meet the ownership conditions over such customers:

i. in the case of a natural person, all the names and surnames, in the original and/or transliteration of such data;

ii. in the case of a legal person, the registered name of the legal person, in the original and/or transliteration of such data;

iii. in the case of a natural person, legal person, body or entity:

- any other names, aliases or trade names where they differ from the registered name;
- digital wallet addresses, where available in the lists of targeted financial sanctions.

Obliged entities may perform manual checks of information subject to screening under this point only where manual checks are proportionate to the size, business model, complexity, or nature of their business.

(b) in case of a match, the information under point (a) shall be checked against all available due diligence information on the customer, the beneficial owners or entities or persons which control or meet the ownership conditions under Article 20(1), point (d), of Regulation (EU) 2024/1624 to determine whether a person is the intended target of the targeted financial sanctions. In case of doubt, the obliged entity shall refer to all other sources available to them, including public sources of information, such as registers of owned and controlled entities and central registers.

(c) regularly screen their customers, beneficial owners and entities or persons which control or meet the ownership conditions under Article 20(1), point (d), of Regulation (EU) 2024/1624, at least under the following circumstances:

i. during customer onboarding or before entering into a business relationship or performing an occasional transaction;

ii. when there is a change in any of the existing designations, or a new designation is made pursuant to Article 26(4) of Regulation (EU) 2024/1624;

iii. there is a significant change in the due diligence data of an existing customer, beneficial owner or entity, or person which controls or meet the ownership conditions under Article 20(1), point (d), of Regulation (EU) 2024/1624, such as but not limited to a change of name, residence, or nationality or change of business operations, which may have a potential impact on the designation as a listed person, body or entity;

(d) ensure that the screening and verification are performed without undue delay by using updated targeted financial sanctions lists.

Section 8

Risk factors associated with features of electronic money instruments

Article 31 - Risk factors

Where supervisors decide to allow for an exemption under Article 19(7) Regulation (EU) 2024/1624, based on the conditions listed in Article 19(7), points (a) to (d), of Regulation (EU) 2024/1624, supervisors shall consider one or more of the following risk factors to determine the extent of that exemption:

(a) the extent to which the payment instrument has low transaction limits or thresholds to limit transaction values;

(b) the extent to which the issuer can verify that the funds originate from an account held and controlled solely or jointly by the customer at an EEA-regulated credit or financial institution;

(c) the extent to which the payment instrument is issued at a nominal or no charge;

(d) the nature and the range of the goods or services that can be acquired, including the level of risks associated with these goods and services;

(e) the extent to which the payment instrument is valid in one or multiple Member States and its issuer is regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer;

(f) the extent to which the transactions through the electronic money instrument are executed by an obliged entity that applies customer due diligence measures and record-keeping requirements laid down in Regulation (EU) 2024/1624;

(g) the extent to which the payment instrument has a specific and limited duration in which the payment instrument can be used;

(h) the extent to which the payment instrument is available through direct channels which may include the issuer or a network of service providers and, in the case of online or non-face-to-face distributions, possess adequate safeguards, including electronic signatures, and anti-impersonation fraud measures;

(i) the extent to which distribution is limited to intermediaries that are themselves obliged entities applying customer due diligence measures and record-keeping requirements laid down in Regulation (EU) 2024/1624;

(j) the extent to which the payment instrument has a limited geographical distribution;

(k) the extent to which the issuer applies adequate technological tools, including geo-fencing and IP tracking, to restrict access from, transfers to or receiving funds from countries that are not EU Member States nor EEA countries.

Section 9

Electronic identification means and relevant qualified trust services

Article 32 - Electronic identification means and relevant qualified trust services

1. Annex I defines the corresponding list of attributes that electronic identification means and qualified trust services are required to feature in accordance with Article 22(6), point (b), of Regulation (EU) 2024/1624, in order to fulfil the requirements of Article 20(1), points (a) and (b), and Article 22(1) of that Regulation, for the purposes of

applying standard and enhanced due diligence measures. Where simplified due diligence is to be applied, the electronic identification means and relevant qualified trust services shall have the corresponding attributes laid down in Annex I that allow compliance with Section 5 of this Regulation.

2. Obliged entities may consider featuring additional attributes to assist the unambiguous identification and verification of the customer or beneficial owner if justified by the ML/TF risk associated with the customer or beneficial owner.

3. Where an electronic identification means or qualified trust service does not possess all attributes that allow the identification and verification of the customer or beneficial owner, as required in Article 22(1) of Regulation (EU) 2024/1624 or Section 5 of this Regulation, the obliged entity shall take steps to obtain and verify the missing attributes through other means in line with Article 22(6) of Regulation (EU) 2024/1624.

4. Obliged entities may consider putting in place enhanced measures to complement the mitigation of ML/TF risks, including the use of higher assurance levels or complementing electronic identification means with qualified trust services.

Article 33 – Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

In cases where the customer has entered into a business relationship before the publication date of this Regulation, the obliged entity shall update the information referred to in Article 23 within five years of publication of this Regulation in the Official Journal of the European Union, by taking into account the risk profile of the customer.

It shall apply from [*Date of application*].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President

[For the Commission
On behalf of the President]
[Position]

ANNEX I: List of attributes referred to in Section 9

	Article 22(1)	Minimum corresponding attributes[8]
(a) for a natural person	(i) all names and surnames	• **family_name** • **given_name**
	(ii) place and full date of birth	• **birth_date** • **birth_place**
	(iii) nationalities, or statelessness and refugee or subsidiary protection status where applicable, and national identification number, where applicable	• **nationality** • **Other** existing attributes covering statelessness and refugee or subsidiary protection status (where applicable) • **personal_administrative_number** (where applicable)
	(iv) the usual place of residence or, if there is no fixed residential address with legitimate residence in the Union, the postal address at which the natural person can be reached and, where available the tax identification number	• **resident_country** • **resident_state** • **resident_city** • **resident_postal_code** • **resident_street** • **resident_house_number** • **resident_address** • **Other** existing attributes covering the tax identification code (where available)
(b) for a legal entity	(i) legal form and name of the legal entity	• **current legal name** • **Other** existing attributes covering legal form • **a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time**
	(ii) address of the registered or official office and, if different, the principal place of business, and the country of establishment	• **current address** • **Other** existing attributes covering additional addresses • **Other** existing attributes covering the country of creation
	(iii) the names of the legal representatives of the legal entity as well as, where available, the registration number, tax identification number and Legal Entity Identifier	• **Other** existing attributes covering the names of the legal representatives of the legal entity • **Legal Entity Identifier (LEI)** (where available) • **VAT registration number** or **tax reference number** (where available)

[8] Based on Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets

		• **Other** existing attributes covering the registration number (where available)
	(iv) the names of persons holding shares or a directorship position in nominee form, including reference to their status as nominee shareholders or directors	• **Other** existing attributes covering the names of persons holding shares or a directorship position in nominee form, including reference to their status as nominee shareholders or directors

2.4 Draft RTS on pecuniary sanctions, administrative measures and periodic penalty payments under Article 53(10) of Directive (EU) 2024/1640

COMMISSION DELEGATED REGULATION (EU) …/...

of XXX

supplementing Directive (EU) 2024/1640 of the European Parliament and of the Council with regards to regulatory technical standards specifying indicators to classify the level of gravity of breaches, criteria to be taken into account when setting the level of pecuniary sanctions or applying administrative measures, and the methodology for the imposition of periodic penalty payments for the purposes of Article 53(10)

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849, and in particular Article 53(10), first subparagraph points (a), (b) and (c) thereof,

Whereas:

(1) Supervisors should have a common understanding of the breaches that warrant the imposition of pecuniary sanctions or administrative measures to ensure a consistent approach to enforcement across Member States. To achieve this, this Regulation sets out a list of indicators that supervisors should take into account when assessing the level of gravity of breaches. It also classifies the level of gravity of breaches into four categories of increased severity.

(2) When determining the level of gravity of breaches by classifying them into the four categories, and when setting the level of pecuniary sanctions and applying administrative measures, supervisors should take into account in their overall assessment all applicable indicators and criteria. Supervisors should use their supervisory judgement to analyse whether and to what extent these indicators and criteria are met.

(3) The list of indicators and criteria specified by this Regulation is non-exhaustive. This is to enable supervisors to take into account the specific context in which the breach has occurred. Where supervisors consider additional specific indicators or criteria, they should justify their use. Supervisors should ensure that supervisory judgement is applied in a coherent and consistent way, with comparable outcomes. They should

also ensure their approach supports the convergence of practices and the consistency and comparability of enforcement outcomes across Member States.

(4) To ensure a consistent approach to assessing the level of gravity of breaches across Member States, this Regulation sets specific combinations of indicators that, if identified by the supervisor as an outcome of the assessment of a breach, should lead to its classification into a certain category of gravity. Those combinations of indicators are not exhaustive. Supervisors may classify other combinations of indicators into the same categories.

(5) An important indicator for classifying the level of gravity of breaches is the conduct of the natural person or of the legal person, including its senior management and its management body in its supervisory function. Supervisors should consider whether a breach was committed intentionally or negligently. Supervisors should pay particular attention to situations where the natural person or legal person appears to have had knowledge of the breach and took no action, or where their action directly contributed to the breach.

(6) Some administrative measures are more severe than others. To ensure a consistent approach across Member States, it is necessary to set out common criteria that supervisors should take into account when considering whether to apply the administrative measures listed under Article 56(2), points (e), (f), and (g), of Directive (EU) 2024/1640, including the withdrawal or suspension of the authorisation, since these could have the highest impact on the obliged entities and the market.

(7) Periodic penalty payments are a tool that supervisors can use to compel compliance with administrative measures. Where supervisors decide to impose periodic penalty payments they should take into account all relevant factors when determining the appropriate and proportionate amount of periodic penalty payments on obliged entities and natural persons to compel them to comply with the imposed administrative measures.

(8) The decision on the imposition of periodic penalty payments should be taken on the basis of findings that allow the supervisor to conclude that an obliged entity or natural person has failed to comply with an administrative measure within a specified period.

(9) Decisions to impose periodic penalty payments should be based exclusively on grounds on which the obliged entity or natural person has been able to exercise its right to be heard.

(10) The periodic penalty payments imposed should be effective and proportionate, having regard to the circumstances of the specific case.

(11) To ensure legal certainty, if not otherwise stipulated by this Regulation, provisions of law applicable in the Member State where the periodic penalty payment is imposed and collected, should apply.

(12) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the Authority for Anti-Money Laundering and Countering the Financing of Terrorism.

HAS ADOPTED THIS REGULATION:

Section 1

Indicators for the classification of the gravity of breaches

Article 1 - Indicators to classify the level of gravity of breaches

To classify the level of gravity of a breach, supervisors shall take into account all of the following indicators, to the extent that they apply:

(a) the duration of the breach;

(b) the repetition of the breach;

(c) the conduct of the natural person or legal person that committed, permitted or did not prevent the breach;

(d) the impact of the breach on the obliged entity, by assessing:

  i. whether the breach concerns the obliged entity and whether it has an impact at group level or any cross-border impact;

  ii. the extent to which the products and services are affected by the breach;

  iii. the approximate number of customers affected by the breach;

  iv. the extent to which the effectiveness of the AML/CFT systems, controls and policies are affected by the breach;

(e) the impact of the breach on the exposure of the obliged entity, or of the group to which it belongs, to money laundering and terrorist financing risks;

(f) the nature of the breach, by assessing whether the breach is related to internal policies, procedures and controls of the obliged entity, customer due diligence, reporting obligations or records retention;

(g) whether the breach could have facilitated or otherwise led to criminal activities as defined in Article 2(1), point (3), of Regulation (EU) 2024/1624;

(h) whether there is a structural failure within the obliged entity with regards to AML/CFT systems, controls or policies or a failure of the entity to put in place adequate AML/CFT systems, controls or policies;

(i) the actual or potential impact of the breach on the financial viability of the obliged entity or of the group of which the obliged entity is part;

(j) the actual or potential impact of the breach:

  i. on the integrity, transparency and security of the financial system of a Member State or of the Union as a whole, or on the financial stability of a Member State or of the Union as a whole;

ii. on the orderly functioning of the financial markets;

(k) the systematic nature of the breach;

(l) any other indicator identified by the supervisors.

Article 2 - Classification of the level of gravity of breaches

1. When classifying the level of gravity of a breach, supervisors shall use four categories as follows, by increased order of severity: category one, category two, category three, category four.

2. To classify the breaches into one of the four categories listed in paragraph 1, supervisors shall assess whether and to what extent all the applicable indicators of Article 1 of this Regulation are met.

3. Supervisors may classify under those categories breaches other than those described in paragraphs 4 to 7.

4. Supervisors shall classify the breach under category one breaches where there is no direct impact or the impact is minor on the obliged entity when assessing the indicators specified in Article 1, points (d) and (e), and, at the same time:

   - when assessing the indicator specified in Article 1, point (a), the breach has lasted for a short period of time, and
   - when assessing the indicator specified in Article 1, point (b), the breach has been committed on a non-repetitive basis.

   Supervisors shall not classify a breach as category one if indicators specified in Article 1, points (g) to (k) are met.

5. Supervisors shall classify the breach as category two where, for the indicators specified in Article 1, points (d) or (e), the impact is moderate and none of the indicators (g) to (k) of Article 1 are met.

6. Supervisors shall classify the breach as at least category three where, for the indicators specified in Article 1, point (d) or point (e), the impact is significant and at the same time:

   (a) when assessing the indicators specified in Article 1, point (a), the breach has persisted over a significant period of time, or

   (b) one of the indicators specified in Article 1 points (b) or (k), is met.

7. Supervisors shall classify the breach as category four where:

   (a) when assessing the indicators specified in Article 1, point (d) or point (e), the impact is very significant, or

   (b) when indicator specified in Article 1, point (h), is met, or

   (c) when assessing the indicator specified in Article 1, point (g), the breach has facilitated or otherwise led to significant criminal activities as defined in Article 2(1), point (3), of Regulation (EU) 2024/1624, or

   (d) when assessing the indicators specified in Article 1, point (i) or (j), the breach has a significant impact.

8. Breaches that would not be classified as category three or category four when assessed in isolation could amount to a breach of category three or four when assessed in combination.

Article 3 - Legal effect of the classification of level of gravity of breaches

A breach with a level of gravity classified as category three or four in accordance with Article 2 shall be deemed serious, repeated or systematic in the meaning of Article 55(1) of Directive (EU) 2024/1640.

Section 2

Criteria to be taken into account when setting the level of pecuniary sanctions and applying the administrative measures listed under this Regulation

Article 4 - Criteria to be taken into account when setting the level of pecuniary sanctions

1. To set the level of pecuniary sanctions, supervisors shall, after performing the assessment of the indicators specified in Articles 1 and 2, take into account:
   (a) the circumstances referred to in Article 53(6) of Directive (EU) 2024/1640, and
   (b) the criteria specified in paragraphs 2 to 6.
2. The level of pecuniary sanctions shall decrease taking into account each of the following criteria, to the extent that they apply:
   (a) the level of cooperation of the natural person or the legal person held responsible with the supervisor. Supervisors shall consider, in particular, whether the natural person or the legal person has quickly and effectively brought the complete breach to the supervisor's attention and whether it has actively and effectively contributed to the investigation of the breach conducted by the supervisor;
   (b) the conduct of the natural person or the legal person held responsible since the breach has been identified either by the natural person or legal person itself or by the supervisor. Supervisors shall consider, in particular, whether the natural person or legal person held responsible has taken effective and timely remedial actions to end the breach or has taken voluntary adequate measures to effectively prevent similar breaches in the future;
   (c) any other criteria identified by the supervisor.
3. The level of pecuniary sanctions shall increase taking into account each of the following criteria, to the extent that they apply:
   (a) the level of cooperation of the natural person or the legal person held responsible with the supervisor. Supervisors shall consider, in particular, whether the natural or legal person has failed to cooperate with the supervisor, did not disclose to the supervisor anything the supervisor would have reasonably expected, or took actions aimed at partially or fully concealing the breach to the supervisor or at misleading the supervisor;

(b) the conduct of the natural person or the legal person held responsible since the breach was identified either by the entity itself or by the supervisor and the absence of remedial actions or measures taken to prevent breaches in the future;

(c) the degree of responsibility of the natural person or legal persons held responsible and whether the breach was committed intentionally;

(d) the benefit derived from the breach insofar as it can be determined and whether the natural person or legal person held responsible has benefited or could benefit either financially or competitively from the breach or avoid any loss;

(e) the losses to third parties caused by the breach, insofar as they can be determined, and the loss or risk of loss caused to customers or other market users;

(f) previous breaches by the natural person or the legal person held responsible and whether the supervisor has imposed any previous sanction concerning an AML/CFT breach or has previously requested remedial action be taken concerning an AML/CFT breach, and whether such action has not been taken in the time requested;

(g) any other criteria identified by the supervisor.

4. In addition to the criteria set out in paragraphs 1 to 3, when setting the level of pecuniary sanctions for natural persons who are not themselves obliged entities, supervisors shall take into account, where applicable, their role and effective responsibilities in the obliged entity, the scope of their functions and the extent of involvement in the breach.

5. When setting the level of pecuniary sanctions, supervisors shall take into account the financial strength of the legal person held responsible, including, where applicable, and in the light of its total annual turnover, any available relevant information from the financial statements in order to assess financial capacity and information from prudential authorities on the level of regulatory capital and liquidity requirements.

6. When setting the level of pecuniary sanctions, supervisors shall take into account the financial strength of the natural persons held responsible by assessing all the information made available. Such assessment shall cover the annual income, whether consisting of fixed or variable remuneration, received from the obliged entity or group of which the obliged entity is part and where relevant, other income of the natural person held responsible.

Article 5 - Criteria to be taken into account when applying the administrative measures listed under this Regulation

1. To set the type of administrative measure, supervisors shall, after assessing the indicators specified in Article 1 and 2, take into account:

(a) the circumstances referred in Article 53(6) of Directive (EU) 2024/1640, and

(b) the criteria specified in paragraphs 2 to 4.

2. When considering whether to restrict or limit the business, operations or network of institutions comprising the obliged entity, or requiring the divestment of activities as referred to in Article 56(2), point (e), of Directive (EU) 2024/1640, supervisors shall take into account each of the following criteria, to the extent that they apply:

(a) the level of gravity is classified pursuant to Article 2 as category three or four;

(b) whether such a measure is capable of mitigating the actual impact or preventing a potential impact by assessing the indicators specified in Article 1, points (e), (g), (i) or (j);

(c) the extent to which the business, operations or network of institutions comprising the obliged entity are affected by the breach or the potential breach;

(d) the extent to which the measure could have a negative impact on customers or stakeholders;

(e) any other criteria identified by the supervisor.

3. When considering whether to withdraw or suspend an authorisation as referred to in Article 56(2), point (f), of Directive (EU) 2024/1640, supervisors shall take into account each of the following criteria, to the extent that they apply:

(a) the level of gravity is classified pursuant to Article 2 as category three or four;

(b) whether such a measure is capable of mitigating the actual impact or preventing a potential impact by assessing the indicators specified in Article 1, points (e), (g), (i) or (j);

(c) the conduct of the natural person or legal person held responsible;

(d) whether there is a structural failure within the obliged entity, with regards to AML/CFT systems and controls and policies or a failure of the entity to put in place adequate AML/CFT systems and controls;

(e) any other criteria identified by the supervisor.

4. When considering the need for a change in the governance structure as referred to in Article 56(2), point (g), of Directive (EU) 2024/1640, supervisors shall take into account each of the following criteria to the extent that they apply:

(a) the level of gravity is classified pursuant to Article 2 as category three or four;

(b) the conduct of the natural person or legal person held responsible;

(c) the natural person or legal person held responsible has not cooperated with the supervisor or took actions aimed at partially or fully concealing the breach to the supervisor or at misleading the supervisor, or the absence of remedial actions since the breach was identified, either by the natural person of legal person held responsible or by the supervisor;

(d) the internal policies, procedures and controls put in place by the obliged entity are ineffective;

(e) any other additional information, where appropriate, including information from an financial intelligence unit, from a prudential supervisor or any other authority or from a judicial authority;

(f) any other criteria identified by the supervisor.

Section 3

Methodology for the imposition of periodic penalty payments pursuant to Article 57 of Directive (EU) 2024/1640

Article 6 - General provision

1. Unless otherwise stipulated by this Regulation and Directive (EU) 2024/1640, the administrative process of the imposition and collection of periodic penalty payments as set out in Article 57 of the Directive (EU) 2024/1640 shall be governed by provisions stipulated by national law in force in the Member State where the periodic penalty payments are imposed and collected.
2. References made to Directive (EU) 2024/1640 shall be construed as references to laws, regulations and administrative provisions into which Member States shall transpose this Directive pursuant to Article 78 thereof.

Article 7 - Statement of findings and right to be heard

1. Before making a decision to impose a periodic penalty payment pursuant to Article 57 of Directive (EU) 2024/1640, supervisors shall submit a statement of findings to the natural person or legal person concerned, setting out the reasons for justifying the imposition of the proposed periodic penalty payment and the amount to be used for its calculation.
2. The statement of findings shall set a time limit of up to four weeks within which the natural person or legal person concerned may make written submissions.
3. The supervisor shall not be obliged to take into account written submissions received after the expiry of that time limit for deciding on the periodic penalty payment.
4. The right to be heard of the natural person or legal persons concerned shall be fully respected in compliance with the administrative process specified in Article 6(1).

Article 8 - Decision on periodic penalty payments

1. The decision on the imposition of periodic penalty payments shall be based only on facts on which the natural person or legal person concerned has had an opportunity to exercise its right to be heard.
2. A decision on the imposition of a periodic penalty payment pursuant to Article 57 of Directive (EU) 2024/1640 shall at least indicate the legal basis, the reasons for the decision and the amount that will be used for the calculation of the final accrued amount of the periodic penalty payment.
3. When deciding on the amount that will be used for the calculation of the final accrued amount of the periodic penalty payment, the supervisor shall take into account all of the following factors:
   (a) the type and the object of the applicable administrative measure that has not been complied with;
   (b) reasons for the non-compliance with the applicable administrative measure;

(c) the losses to third parties caused by the non-compliance with the applicable administrative measure, provided they were determined when the applicable administrative measure was imposed;

(d) the benefit derived from the non-compliance with the applicable administrative measure, provided they were determined when the applicable administrative measure was imposed;

(e) the financial strength of the natural person or legal person concerned, provided this was determined when the applicable administrative measure was imposed.

Article 9 - Calculation of periodic penalty payments

1. The amount of the periodic penalty payment can be set on a daily, weekly or monthly basis.

2. A periodic penalty payment shall be enforced and collected only for the period of non-compliance with the relevant administrative measure referred to in Article 56(2), points (b), (d), (e) and (g), of Directive (EU) 2024/1640. The period of non-compliance with the relevant administrative measure referred to in Article 56(2), points (b), (d), (e) and (g), of Directive (EU) 2024/1640 shall be determined by the supervisor.

Article 10 - Limitation period for the collection of periodic penalty payments

1. The collection of the periodic penalty payment shall be subject to a limitation period of five years. The five years period referred to in paragraph 1 shall start to run on the day following that on which the decision setting the final accrued amount of periodic penalty payment to be paid is notified to the natural person or legal person concerned.

2. The limitation period for the collection of periodic penalty payments can be interrupted or suspended in compliance with provisions stipulated by national law in force in the Member State where the periodic penalty payments are collected.

Article 11 - Entry into force and application date

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from [*Date of application*].

It shall not apply to proceedings related to pecuniary sanctions, administrative measures and periodic penalty payments initiated before 10 July 2027.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President
[…]

On behalf of the President
[…]
[Position]

3. Technical advice

3.1 Technical advice on base amounts for pecuniary sanctions

95. The mandate for the adoption of these guidelines is Article 53(11) of Directive (EU) 2024/1640 (AMLD6).

96. Pursuant to the mandate, AMLA shall issue, by 10 July 2026, guidelines on the base amounts for the imposing of pecuniary sanctions relative to turnover, broken down per type of breach and category of obliged entities (guidelines on base amounts).

97. The mandate for the EBA to issue its technical advice is the March 2024 Call for Advice of the EC, which stated that the provision of such advice by the EBA is optional and not mandatory.

98. The EBA has used its work stream set up for the purposes of discussing a draft for RTS on pecuniary sanctions, administrative measures and periodic penalty payments under Article 53(10) AMLD6 to discuss the aspects of the mandate for guidelines on base amounts.

99. Based on discussions with the respective work stream, subgroup and AMLSC, the EBA is delivering the following technical advice to the EC of the European Union on the guidelines on base amounts.

Scope and addresses of the guidelines on base amounts

100. It is the understanding of the EBA that the addressees of the guidelines on base amounts should be both the national competent authorities (NCAs) and the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), when deciding on the imposition of pecuniary sanctions for breaches committed by obliged entities.

101. The EBA would recommend that the guidelines on base amounts apply to all breaches of obligations to which obliged entities are bound under the new AML/CFT framework[9], including national provisions into which Member States transpose the requirements stipulated by AMLD6, for which both NCA's and the AMLA can impose pecuniary sanctions.

102. in the case of obliged entities, it is the EBA's understanding that the mandate under Article 53(11) AMLD6 covers not only legal persons, but also natural persons who themselves are recognised under the AML/CFT framework.

[9] Regulation (EU) 2024/1620, OJ L, 2024/1620, 19.6.2024 (AMLAR); Regulation (EU) 2024/1624, OJ L, 2024/1624, 19.6.2024 (AMLR); Directive (EU) 2024/1640, OJ L, 2024/1640, 19.6.2024 (AMLD); Regulation (EU) 2023/1113, OJ L 150, 9.6.2023 (FTR).

103. Furthermore, in the case of natural persons, it is the EBA's understanding, that the guidelines on base amounts should cover not only natural persons that are themselves obliged entities but also in compliance with Article 53(4) AMLD6, senior management members and other natural persons who under national law are responsible for the breach of obligations stipulated by the AML/CFT framework.

Interplay between the guidelines on base amounts and certain AMLD6 provisions

104. When developing the guidelines on base amounts, particular attention needs to be focused on the understanding of the new AML/CFT legal framework.

105. The new guidelines on base amounts must respect the existing AMLD6 provisions, especially Chapter IV, Section IV, AMLD6 (Article 53, Article 55). The future guidelines must also be compliant with the future regulatory technical standards that shall be adopted under Article 53(10) AMLD6.

Interpretation of terms used in the mandate of the guidelines for base amounts

106. Based on discussions held with NCAs and the EC, it is the understanding of the EBA that the following terms included in the mandate of the guidelines on base amounts should be interpreted as follows:

Base amount – these term should be understood as a range rather than a specific amount for a specific type of a breach and category of an obliged entity. Furthermore, the range of base amounts needs to reflect the category of the obliged entity, the type of breach and the turnover of the obliged entity. It is the view of the EBA that, besides the criterion of turnover of the obliged entity, further criteria should be taken into consideration, e.g. volume of assets, own funds ratios, etc.

It is necessary to point to the fact that the term base amount does not refer to the final amount of a pecuniary sanction. As AMLD6 provides for flexibility to NCAs and the AMLA to determine the final amount of a pecuniary sanction, the aim of the guidelines should be to determine the starting range of amounts to be used for the imposition of pecuniary sanctions per type of a breach of an obligation stipulated by the AML/CFT framework.

Type of breach – there has been an agreement, that this term should be connected to the categorisation of breaches as proposed by the draft RTS under Article 53(10) AMLD6; thus each breach should be categorised as a category 1 to 4 breach.

There is an agreement among AMLSC members that it would be over prescriptive to include in the guidelines on base amounts a nomenclature of all possible breaches under the AML/CFT framework and to attach to each of such breaches a specific base amount. Such an approach could undermine the approach of AML/CFT supervisors to exercise their powers to impose pecuniary sanctions in compliance with the provisions stipulated by Article 55 (3) to (5) AMLD6.

Category of obliged entity – there has been an agreement that this term should be understood as 'types' of obliged entities, as provided for in Article 3 AMLR. Based on discussions held with the AMLSC, it is the EBAs understanding, that at this point in time, it could be counterproductive to group obliged entities into specific groups, e.g. to group financial vs. non-financial obliged entities, as there are significant differences in the business models and risk profiles of different types of financial and non-financial obliged entities.

Turnover - there has been an agreement, that this term should cover both the turnover of an obliged entity that is a legal person, as well as the income of a natural person, that may be subject to pecuniary sanctions under the AML/CFT framework, in order to ensure compliance with the provisions of Article 53(6), point d) and 55 (3), point (b) AMLD6.

107. in the case of the term turnover of obliged entities that are legal persons, it is the EBAs understanding that this term refers to the 'total annual turnover' of that obliged entity (see Article 55(3), point (a), AMLD6) and that amount should be provided by the latest available financial statements prepared in compliance with the relevant accounting standards and approved by the management body of the obliged entity, or should come from the latest available consolidated accounts approved by the management body of the ultimate parent undertaking.

108. In the absence of the latest financial statements or consolidated accounts of a legal person or income of a natural person, the guidelines on base amounts should provide for alternative solutions for the AML/CFT supervisor to determine the base amount.

Date of application of the guidelines on base amounts

109. The guidelines on base amounts shall be issued by 10 July 2026. It is the understanding of the EBA that the guidelines should apply from 10 July 2027, as this is the deadline for Member States to bring into force the laws, regulations and administrative provisions necessary to comply with the provisions AMLD6.

3.2 Technical advice on group-wide policies and procedures

110. Article 16(4) of Regulation (EU) 2024/1624 (AMLR) mandates AMLA to draft RTS specifying minimum standards for group-wide policies and procedures, including:

a. minimum standards for information sharing within the group;

b. the criteria for identifying the parent undertaking for groups whose head office is located outside of the Union[10]; and

c. the conditions under which the provisions of Article 16 AMLR apply to entities that are part of structures which share common ownership, management or compliance control, including networks or partnerships, as well as the criteria for identifying the parent undertaking in the Union in those cases.

111. The EC, in its CfA, asked the EBA to propose options that AMLA could consider when taking this mandate forwards, to the extent that this was possible in light of the resources the EBA had available.

112. In preparing these options, the EBA drew on information from its prudential work and AML/CFT guidelines or standards where applicable. Aspects of group-wide policies and procedures that are covered by AMLA's mandates in Articles 9(4) and 10(4) AMLR fall outside of the scope of this technical advice and have not been considered. This technical advice focuses on minimum standards for information sharing within groups that are financial institutions.

Rationale

113. Sharing information within the group supports the effective identification and management of ML/TF risk. It also makes effective group AML/CFT supervision possible. Since information shared in the AML/CFT context can be sensitive and consist of personal data, it should be subject to sufficient safeguards and compliant with the requirements of the GDPR[11], EUDPR[12], and the new AML/CFT framework[13]. Accordingly, the parameters within which entities within a group should be able to exchange information and process such information should be clearly defined.

Minimum standards for information sharing within the group

114. Minimum standards for information exchange within a group should include provisions governing the acceptable use of information ('why'), provisions that specify the nature of the information that can be exchanged ('what') and provisions relating to the way information is shared ('how').

[10] See Article 2(1), point (42)(b), AMLR.

[11] Regulation (EU) 2016/679, OJ L 119, 4.5.2016, p. 1. (GDPR).

[12] Regulation (EU) 2018/1725, OJ L 295, 21.11.2018, p. 39. (EUDPR).

[13] Chapter VII of Regulation (EU) 2024/1624 (AMLR), Chapter VI of Directive (EU) 2024/16 AMLD6), Article 98 of Regulation (EU) 2024/1620 (AMLAR).

Acceptable use of information

115. The processing of personal data for the purpose of ML/TF prevention is necessary for the performance of a task carried out in the public interest and in line with the AML/CFT package[14].

116. For entities that belong to a group, having access to personal data from individual customers that are also served elsewhere in the group is key to the effective identification and management of ML/TF risk. This may include information that members of a group have obtained through a partnership for information sharing. At the same time, it is important that the risk of unintended consequences of such information sharing, for example unwarranted de-risking, be mitigated.

Risk assessments

117. The use of personal data for AML/CFT purposes needs to be clearly defined to provide a legal basis for the exchange of such data, particularly in situations where a group may not be based exclusively in the EU. The RTS could limit the use of personal information shared within the group to customer risk assessments or extend it to business-wide risk assessments, too.

118. Limiting the use of personal information to individual customer risk assessments will ensure that customers' personal data can be shared within the group to inform customer risk assessments. However, under such an approach, the use of personal data for any other purpose might not be permitted.

119. Customer data may also be helpful in informing the business-wide risk assessment and ultimately, the group's ML/TF risk assessment, making them more comprehensive and accurate. Permitting the use of personal data for a sufficiently broad range of ML/TF risk assessments also appears to be in line with the provisions of Article 16(1), first and second subparagraph, AMLR, Article 9(2)(a) AMLR and the mandate in Article 10(4) AMLR, and aligns with established practices, including:

a. Guidelines EBA/GL/2022/05 on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849;
b. Guidelines EBA/GL/2024/14 on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures; and
c. Guidelines EBA/GL/2021/05 on internal governance under Directive 2013/36/EU.

120. Adopting a broad view of possible uses of shared personal data and reflecting this in the draft RTS is therefore the preferred option.

[14] See Article 98(1) of Regulation (EU) 2024/1620 (AMLAR) in connection with Article 70 AMLD6 and Article 76 AMLR.

Information from partnerships for information sharing

121. Article 75 AMLR specifies which information can be exchanged between members of a partnership for information sharing. Information received from a partnership should not be further transmitted, except in certain circumstances as stipulated in Article 75(5) AMLR, such as when included in a report submitted to the FIU, provided to the AMLA, or requested by law enforcement or judicial authorities.

122. Article 75 AMLR does not set out in detail how information could be shared across borders. Achieving cross-border sharing of information will require consensus among different data protection authorities and must address challenges like data localisation. Article 75 states that 'Responsibility for compliance with requirements under Union or national law shall remain with the participants in the partnership for information sharing.'

123. In the absence of specific provisions in Article 75 AMLR, the RTS could include provisions on the onward sharing of information received on the basis of Article 75 AMLR within the group. This could be justified because information obtained through partnerships may affect the group's understanding and assessment of ML/TF risk and therefore, may need to be shared across the group. At the same time, further analysis would be warranted to ensure that provisions of Article 75, such as record keeping and restrictions on onward sharing, be respected.

Consumer protection and de-risking

124. Access to financial services is an important public interest goal. As such, it is important that AML/CFT measures do not lead to institutions unfairly denying customers access to financial services. The EBA issued guidelines on tackling de-risking in 2023[15].

125. Information sharing within a group may lead an entity to take a decision to de-risk customers even if those customers do not present higher ML/TF risks for the purposes of their business relationship with that entity. This could be the case, for example, because other group entities have assessed them as high ML/TF risk or because they have been named in an STR.

126. The draft RTS could contain provisions to specify the responsible use of information shared within the group to prevent such unwarranted de-risking. Alternatively, relevant provisions could be set out in another technical norm issued by AMLA under a different mandate. Examples of mandates that could be used include the mandate under Article 21 AMLR to issue joint guidelines, together with the EBA and by 10 July 2027, on ensuring customers' access to at least basic payment services.

127. Though less binding than including provisions in RTS, AMLA could set clear expectations in such guidelines regarding the steps obliged entities should take to avoid unwarranted de-risking. Furthermore, addressing issues in RTS for which a guidelines mandate exists could mean that provisions in guidelines may become legally binding. For this reason, including de-risking provisions

[15] EBA/GL/2023/04 - Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services.

in the group information sharing context in guidelines under Article 21 AMLR is the preferred option.

Information to be shared within the group

128. According to Article 16(3), first subparagraph, AMLR, the sharing of information within the group shall cover:

a. the identity and characteristics of the customer, its beneficial owners or the person on behalf of whom the customer acts;

b. the nature and purpose of the business relationship and of the occasional transactions; and

c. the suspicions, accompanied by the underlying analyses, that funds are the proceeds of criminal activity or are related to terrorist financing reported to the FIU pursuant to Article 69, unless otherwise instructed by the FIU.

Identity and characteristics of the customer, beneficial owner or person on behalf of whom the customer acts

129. The information that group entities should be able to share on the identity and characteristics of the customer, beneficial owner or person on behalf of whom the customer acts could be defined broadly and encompass all information set out in the draft RTS under Article 28(1) AMLR. Alternatively, the RTS could restrict information to that which is set out in Article 75 AMLR.

130. Opting for a broad definition would require group entities to share relevant information about all customers, beneficial owners and persons on behalf of whom the customer may act, as necessary and irrespective of the level of ML/TF risk associated with the business relationship. It would allow all group entities that serve the customer to obtain a comprehensive view of the risks associated with it. To ensure that personal data are protected, the information should be accessible only on a need-to-know basis to entities that require it for the purposes of CDD and the performance of ML/TF risk management.

131. Article 75 AMLR on the exchange of information within partnerships for information sharing limits the type of information that can be shared. For example, under this article, the sharing of information is conditional upon the customer being associated, or suspected of being associated, with a higher ML/TF risk. Adopting a similar approach for the purpose of the mandate in Article 16(4) AMLR would present advantages in terms of data protection, but might significantly reduce the AML/CFT potential of group-wide information sharing. This is because group entities would not be able to obtain a single view of most customers and may miss important ML/TF warning signals associated with a customer's behaviour or transaction activities. Furthermore, the same customer can carry different levels of risk in different business relationships.

132. Article 75 AMLR restricts information sharing because obliged entities that participate in a partnership may not be part of the same group. The same considerations therefore do not apply to situations within the scope of Article 16 AMLR. This suggests that information sharing among

obliged entities that are part of the same group, and bound by the same group-wide AML/CFT policies, should be broadly defined.

Nature and purpose of business relationships and of occasional transactions

133. The information group entities should be able to share in relation to the nature and purpose of the business relationship or occasional transaction could be extensive and encompass all information set out in the draft RTS under Article 28(1) AMLR. Alternatively, it could be limited to that set out in Article 75 AMLR.

134. Providing that group entities are able to share all relevant information on the nature and purpose of a customer's business relationship or occasional transaction would provide group entities that serve the customer with a comprehensive view of the risks associated with it. It would also be in line with the provisions of Article 16(3) AMLR, which specifically refers to the nature and purpose of the business relationship and to occasional transactions in an information sharing context.

135. By contrast, the scope of information that can be shared could be limited to information on the nature and purpose of business relationships established by customers who are associated with higher ML/TF risk in line with provisions in Article 75 AMLR. It could also support the effective protection of personal data.

136. Considering that a complete customer view requires an understanding of all aspects of a customer's behaviour or transactions, including occasional transactions, that the purpose of Article 75 AMLR is different from that stipulated by Article 16 AMLR and that Article 16(3) AMLR does not appear to limit the exchange of data by levels of risk, a broad definition could be adopted. To nevertheless ensure that personal data are protected, the information should be accessible on a need-to-know basis to entities that require it for the purposes of CDD and the performance of ML/TF risk management.

Suspicions activities and transactions

137. Article 16(3), first subparagraph, AMLR requires that group entities share within the group any suspicions, and the analysis underlying this suspicion, that funds are the proceeds of crime or linked to terrorist financing to the extent that such suspicions have been reported to the FIU. This suggests that, in relation to reporting of suspicious transactions (STRs), both the fact that an STR was submitted and the content of an STR should be shared between entities of a group, unless instructed otherwise by the FIU.

138. Paragraph 81, point g) of the Guidelines EBA/GL/2022/05[16] mentions that the group AML/CFT compliance officer should ensure that entities of the group share information that a suspicious transaction report has been filed. Article 5(1), point(b)(ii), of the Commission Delegated Regulation (EU) 2019/758 – RTS on the implementation of group wide AML/CFT policies in third

[16] Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849.

countries requires that, when sharing information related to suspicious transactions within a group, an overview of the circumstances that gave rise to the suspicion, in the form of aggregated statistical data, must be included. Furthermore, Article 5(2) of that Commission Delegated Regulation requires credit institutions and financial institutions to take additional measures set out in provisions of Article 8.

139. The RTS could require that all information relating to an STR be shared, or restrict such information sharing to aspects that are strictly necessary for an entity's ML/TF risk assessment purposes.

140. If information sharing were restricted to aspects that are necessary to enable entities to carry out a risk assessment, the entity that holds the information would have to determine which information would be useful for the receiving entity. This could create legal uncertainty, introduce institutional complexity and hamper the timely identification and management of ML/TF risks.

141. By contrast, a broad approach would entail the sharing of the STR and associated information. This would be in line with Article 8, point (g), of the Commission Delegated Regulation, which provides that it shall be ensured that entities share 'information that gave rise to the knowledge, suspicion or reasonable grounds to suspect that money laundering and terrorist financing was being attempted or had occurred, such as facts, transactions, circumstances and documents upon which suspicions are based, including personal information to the extent that this is possible under the third country's law'. The EBA Q&A 2020/5349 on Article 5, paragraph 1 of Commission Delegated Regulation (EU) 2019/758 further specifies the extent of information to be shared. To comply with Article 73 AMLR related to the prohibition of disclosure, the sharing of information could be performed on a 'need to know' basis and be limited to the persons eligible to have information as defined in the group wide policies and procedures and in accordance with Article 69 and Article 11(2) AMLR.

142. For both approaches, rules governing this information exchange should include provisions for updating the information where necessary, for example in situations where information is received from the FIU, where procedures or investigations within a group are ongoing or closed, or where a suspicion no longer exists. In any case, the sharing of information would have to be performed in accordance with the provisions of Regulation (EU) 2016/679, Regulation (EU) 2018/1725, Chapter VII of Regulation (EU) 2024/1624 (AMLR), Chapter VI of Directive (EU) 2024/1640 (AMLD6) and Article 98 of Regulation (EU) 2024/1620.

Other information that could be exchanged

143. Additional information that could be exchanged in the group context includes:

a. aggregated data that do not include personal data on individual customers, beneficial owners or persons acting on a customer's behalf;

b. information on atypical activity group entities identified while monitoring the customer's transactions and business relationship; and

c. feedback from the FIU on individual STRs; and

d. information on deficiencies in an entity's AML/CFT policies and procedures and associated remediation measures.

144. No restrictions exist in relation to the sharing of information about trends, typologies or other information that does not include information on individual customers or their transactions. Including such a provision in this draft RTS may interact with other AMLA mandates included in Articles 9 and 10 AMLR and will have to be considered in this context.

145. In relation to atypical activity, this could be shared on a case-by-case basis where warranted in light of the potential ML/TF risk. This information could be part of the information addressed in this draft RTS, for example in the context of the exchange of CDD information, as a specific category or as part of the information on a suspicion shared with the FIU, in compliance with Article 69 AMLR.

146. In relation to feedback on STRs, Article 28 AMLD6 requests that FIUs provide feedback on the reporting of suspicions but not on individual STRs. In practice, where feedback on individual STRs is provided, sharing it would be possible only with the express authorisation of the FIU. For this reason, the draft RTS should not be covering this point.

147. In relation to information on deficiencies and remediation measures, this does not encompass personal data, but it is an important part of the ML/TF risk management of a group. According to Guidelines EBA/GL/2022/05[17], the group management body should be informed of supervisory activities carried out in entities of the group by a competent authority, or deficiencies identified and ensure remediation measures are completed by the subsidiary or branch in a timely and effective manner. At the same time, such a provision may interact with other AMLA mandates contained in Articles 9 and 10 AMLR and its inclusion in the RTS will have to be considered in this context.

How to share information

148. Fulfilling the mandate in Article 16(4) AMLR suggests that consideration be given to the way such information is shared. This can relate to specific structures that are put in place, and to the management of specific situations, such as the sharing of information with entities in third countries.

The role of the parent undertaking

149. Article 16(1) AMLR provides that a parent undertaking must ensure that the requirements on internal procedures, risk assessment and staff referred to in Section 1 of Chapter 2 of the AMLR apply at all branches and subsidiaries of the group in the Member States and, for groups whose head office is in the Union, in third countries.

[17] Paragraph 77 a and b of Guidelines EBA/GL/2022/05.

150. In accordance with Article 109(2) of Directive 2013/36/EU, parent undertakings and subsidiaries subject to that directive should ensure that governance arrangements, processes and mechanisms are consistent and well integrated on a consolidated or sub-consolidated basis. To this end, parent undertakings and subsidiaries within the scope of prudential consolidation should implement such arrangements, processes and mechanisms in their subsidiaries that are not subject to Directive 2013/36/EU, including those established in third countries and offshore financial centres, to ensure robust governance arrangements on a consolidated and sub-consolidated basis.

151. Furthermore, Guidelines EBA/GL/2022/05[18] mention that the parent undertaking of a group should ensure the exchange of adequate information between the business lines and the AML/CFT compliance function, and the compliance function where those are different functions, at group level, and between the heads of the internal control functions at group level and the management body of the credit or financial institution. The guidelines also specify that the AML/CFT compliance officer of a subsidiary or branch should have a direct reporting line with the group AML/CFT compliance officer.

152. The draft RTS could specify that the parent undertaking must centralise all information sharing, or adopt a decentralised approach whereby horizontal sharing of information is possible.

153. Requiring a centralised approach to information sharing would entail the parent undertaking setting up arrangements to ensure that all information that is held by group entities and needs to be shared in the AML/CFT context is first provided to it, before being redirected by it to relevant entities within the group. The advantage of this option is that it enables the parent undertaking to have a complete view of the group's AML/CFT activities and risks. It also limits risks related to the processing of sensitive or confidential data. On the other hand, it increases organisational complexity and may make AML/CFT compliance less flexible or responsive.

154. By contrast, a decentralised approach could be conducive to information flowing both vertically and horizontally from subsidiaries or branches to the parent undertaking, from the parent undertaking to subsidiaries or branches, and between subsidiaries and branches themselves. In line with existing approaches and provisions in the AMLR regarding the role of the parent undertaking, the RTS could include provisions to ensure that the group compliance function maintains oversight of information exchanged between different entities of the group.

155. Arrangements for decentralised information sharing may be complex to put in place but could reflect the nature, size and complexity of the group and the way it conducts its business. For example, if shared customers are rare across the group, a manual process may suffice. Where complex relationships are common, or risks are increased, automation may be the only acceptable tool.

156. Special confidentiality requirements, unrelated to AML, may apply to certain information shared with AML/CFT supervisors. For example, some countries' laws may permit sharing such

[18] Paragraphs 76 and 83 of the Guidelines EBA/GL/2022/05.

information with the head office only. Under both approaches, the RTS would have to be drafted in a way to accommodate this.

Data protection

157. Different provisions of Union law in the area of AML/CFT provide that obliged entities can process personal data under conditions stipulated in those acts. The processing of such data is limited to the purpose of the prevention of money laundering and terrorist financing.

158. Should personal data be transferred to entities outside of the EU, the GDPR and EUDPR stipulate conditions that needs to be met. In the AMLR, Article 16(3) provides that parent undertakings of groups that have establishments in third countries need to ensure that the information exchanged is subject to sufficient guarantees in terms of confidentiality, data protection and use of the information, including to prevent its disclosure.

159. The AML/CFT framework needs to abide by the principle of 'data minimisation' of EU data protection rules, as well as the principle of 'proportionality'. Article 3(1) of the GDPR provides that the Regulation applies to processing in the context of the activities of an establishment in the EU 'regardless of whether the processing takes place in the Union or not'. The place of processing is therefore not relevant in determining whether or not the processing, carried out in the context of the activities of an EU establishment, falls within the scope of the GDPR.

160. Any transfer of personal data outside the application of the GDPR or EUDPR is subject to specific provisions contained in Chapter V of those regulations.

161. In light of this, one option would be that the RTS provide that the transfer of personal data to third countries or international organisations takes place on the basis of an adequacy decision (Article 45 of the GDPR, Article 47 of the EUDPR) or is subject to appropriate safeguards (Article 46 of the GDPR, Article 48 of the EUDPR). Alternatively, the second option is that the transfer of personal data to third countries or international organisation could take place on the basis of derogations (49 of the GDPR, Article 50 of the EUDPR).

162. A transfer that is based on derogations can only be performed on a case-by-case basis and is subject to notification duties to data protection supervisors or even to the data subject involved. Since information exchange for customer due diligence and ML/TF risk management is likely to be systematic in nature, an approach that relies on a case-by-case assessment and notifications may not be operationally feasible. This means that Option 1, which avoids this complexity while allowing for systematic information sharing with third countries and the protection of personal data under the applicable EU data protection framework, as further specified by the EU AML/CFT framework, is likely to lead to more effective outcomes.

4. Accompanying documents

The EBA carried out draft cost-benefit analyses of its consultation proposals and updated these analyses in light of the consultation responses it received. It also carried out checks, using data from institutions and AML/CFT supervisors, to test the plausibility of its proposed approaches to entity-level risk assessments and enforcement and amended its proposals where necessary.

Throughout its work, and to the extent that provisions in the AMLD6, AMLR and AMLAR permitted it, the EBA had regard to the principles of a proportionate, risk-based approach that leads to effective and reliable outcomes and keeps the cost of compliance to a necessary minimum.

4.1 Cost-benefit analysis / impact assessment – RTS under Article 40(2) AMLD6 on the assessment of obliged entities' risk profile

A. Problem identification

Between 2018 and 2025, EBA staff reviewed the approach to AML/CFT supervision of all supervisors responsible for supervising the banking sector. The EBA also published four consecutive opinions on the ML/TF risks to which the European financial sector is exposed. The latest opinion was published in July 2025. In 2023, EBA staff also carried out a stock take to identify the similarities and differences between the approaches to the assessment of ML/TF risks developed by supervisors. It found that there was a low degree of convergence between the approaches put in place by supervisors.

The EBA's findings mean that supervisors' entity-level ML/TF risk assessments are not comparable. This impedes AML/CFT supervision, creates significant costs for institutions that operate on a cross-border basis, and makes the EU vulnerable to financial crime. The EBA highlighted this in its 2020 response to the EC's Call for Advice on the future AML/CFT framework.

The EU co-legislators acted on the EBA's advice and included specific provisions in the new AML/CFT legal framework that harmonise supervisors' approaches to assessing entity-level ML/TF risk and make comparable outcomes possible. They also mandated AMLA to further specify in draft RTS the steps supervisors must take in this regard.

B. Policy objectives

In March 2024, the EC asked the EBA to advise it on the content of the RTS to be developed by AMLA pursuant to Article 40(2) of Directive (EU) 2024/1640.

In accordance with Article 40(2), the draft RTS must set out:

- The benchmarks and methodology for assessing and classifying the inherent and residual risk profile of obliged entities;
- The frequency at which these risk profiles must be reviewed.

Article 40(2) of Directive (EU) 2024/1640 also specifies that the frequency at which the risk profiles must be reviewed shall take into account any major events or developments in the management and operations of the obliged entity, as well as the nature and size of the business.

C. Baseline scenario

Under the current legislative framework, the rules pertaining to such assessment are not harmonised at EU level, although common principles exist. These principles are set out in the EBA's risk-based supervision guidelines.

D. Options considered

Quantity of data to be collected

To be able to assess and classify the inherent and residual risk profile under their supervision, supervisors need to collect data from obliged entities and other stakeholders such as prudential supervisors and FIUs.

Regarding the level of granularity and the quantity of data to be collected from these entities and other stakeholders when relevant, and taking into account current supervisory practices in EU Member States, the EBA considered two options:

Option 1a: Collecting an extensive set of data from obliged entities and stakeholders that may go beyond the data points that are strictly necessary for ML/TF risk assessment purposes.

Option 1b: Limiting data requests from obliged entities and stakeholders to those that are strictly necessary for ML/TF risk assessment purposes.

Some EU AML/CFT supervisors collect extensive amounts of data to inform their entity-level risk assessments. For example, in several cases, annual AML/CFT questionnaires contain more than 500 data points.

Collecting an extensive set of data from obliged entities and stakeholders would have the benefit of providing supervisors with comprehensive information about all aspects of each institution's operations and controls environment. On the other hand, evidence from the EBA's implementation reviews shows that, in most cases, supervisors that obtain extensive data sets do not use all data they obtain for the assessment and classification of risks. Feedback from the private sector further suggests that requesting extensive sets of data can create significant costs. As the number of data points supervisors need, and in practice use, for entity-level ML/TF risk assessment purposes is limited, the amount of data collected and required under the draft RTS could thus be limited to that

strictly necessary for ML/TF risk assessment purposes. Importantly, limiting data points for ML/TF risk assessment purposes in this way does not limit supervisors' right to obtain data for on-site and offsite AML/CFT supervision purposes.

In the short term, because of the material differences between the systems put in place by supervisors, the implementation of a harmonised set of data will inevitably lead to changes in the way supervisors request that data, for example AML/CFT periodic questionnaires. These changes may be significant and mean that entities and stakeholders may need to adapt their IT infrastructure to collect and report data that they have not previously collected or reported. However, the implementation of a harmonised set of data collected could ultimately lead to a decrease in entities' and stakeholders' costs and to greater efficiency. For instance, in the medium to long term, it is expected that costs would decrease for entities operating in different Member States because the same data would be collected in all Member States. Additionally, several respondents pointed out that greater harmonisation would be highly beneficial because it was currently difficult to deal with different interpretations of specific AML/CFT concepts across Member States. Therefore, the respondents strongly supported a move towards a harmonised risk assessment methodology.

Based on the above, **Option 1b was chosen as the preferred option** and the EBA proposed in its public consultation that supervisors limit the data they collect from obliged entities and stakeholders to that which is strictly necessary for entity-level ML/TF risk assessment purposes.

Consultation feedback on the extent of data requests

A total of 118 respondents participated in the consultation on these draft RTS. Most of these respondents were credit or financial institutions, or trade associations representing such institutions. A minority of respondents belonged to the non-financial sector (including lawyers, accountants, advisers and non-profit organisations).

Respondents to the consultation identified the scope of data requests as the primary concern. This issue was articulated in three distinct dimensions:

Volume of data points: Many respondents claimed that the quantity of data points required was too high. To address this, the EBA carried out a review of the data points and risk assessment methodology and deleted the number of data points by approximately 15%. It also introduced transition provisions, by opting for a staged approach whereby two data points that respondents suggested were particularly difficult to obtain immediately would be requested only at a later stage, to give more time for firms to adapt to the new framework. It also clarified which data points corresponded to which financial services sector.

Ambiguity of terminology: Respondents suggested that several data points were unclear or difficult to interpret. To address this, the EBA reviewed the description of the data points based on the consultation feedback and, in collaboration with competent authorities and more than 100 institutions, prepared an interpretative note clarifying the definitions and scope of these terms.

Cost of data production: Despite the removal of certain data points, a number of items remain that were consistently flagged as particularly costly or burdensome to produce. Following extensive consultations with competent authorities, the EBA is of the view that these data points are essential for the risk assessment methodology and that therefore the benefits of including them should outweigh the costs.

Use of automated scores to assess risks relating to the effectiveness of controls

All supervisors use objective indicators and automated scores to assess and classify the inherent risks to which obliged entities are exposed. As regards the assessment of the quality of the AML/CFT controls that obliged entities put in place to effectively mitigate these inherent risks, supervisors have implemented different approaches. Some rely entirely on their staff's professional judgement, while others rely on information provided by institutions that feeds an automated controls score. Some supervisors use a combination of automated scores and supervisory judgement.

In line with supervisors' current practice, and considering both the large number of obliged entities in the EU that need to be assessed and the limited resources supervisors have available to carry out this assessment, the EBA considers that an automated assessment of inherent risks is necessary. With regards to the assessment of the quality of controls, the EBA considered three options:

Option 2a: Assessing the quality of controls based entirely on professional judgement.

Option 2b: Assessing the quality of controls based on a two-step process, whereby the control risks would be first assessed in an automated manner based on objective criteria and then manually adjusted based on professional judgement where necessary.

Option 2c: Assessing the quality of controls based entirely on an automated score.

Assessing the quality of controls based entirely on professional judgement based on inspection or offsite supervision findings could make the assessment very accurate for individual institutions. Nevertheless, applying professional judgement to all obliged entities would create significant costs and may require some supervisors to hire additional staff, particularly in situations where they are responsible for the AML/CFT supervision of a large number of obliged entities (several thousands in some cases). In addition, the benefits of assessing the quality of AML/CFT controls based on professional judgement alone may differ from one obliged entity to another, as the extent to which this judgement is reliable would depend on the extent to which the underlying information is complete and up to date; for example benefits could typically be high in cases where an obliged entity has recently been subject to intrusive supervision (such as on-site inspections) but will be lower where obliged entities have not been subject to such actions. As a result, to be effective and sufficiently reliable, the steps supervisors would have to take and the resources that they would need to deploy to keep professional judgements relevant and up to date would not be commensurate with the level of ML/TF risk associated with different entities under their supervision. Finally, until the common supervision methodology envisaged by Article 8 AMLAR is in place and applied, the bases on which supervisors arrive at their professional judgement are likely

to diverge and make comparisons between obliged entities from different Member States more difficult.

Assessing the quality of controls automatically addresses those concerns but carries a risk that mistakes in obliged entities' submissions or deliberate attempts to frustrate the risk assessment process may lead to inadequate outcomes. For this reason, supervisors should be able to override automated controls risk scores using professional judgement. To nevertheless ensure a consistent approach and comparability of risk scores across EU Member States, such adjustments should be possible only in specific circumstances and subject to the application of common criteria.

Based on the above, **Option 2b has been chosen as the preferred option** and the draft RTS on risk assessment and classification of the risk profile of obliged entities will request that supervisors follow a two-step process to assess the quality of the AML/CFT controls, whereby the control risks would be first assessed in an automated manner based on objective criteria and then manually adjusted based on professional judgement where necessary.

Level of granularity of the methodology and benchmarks described in the draft RTS

Article 40(2) of Directive (EU) 2024/1640 provides that the draft RTS must set out the benchmarks and methodology to be used to assess and classify the inherent and residual risk profile of obliged entities but does not prescribe the extent to which these benchmarks and methodology need to be described. In this regard, the EBA considered two options.

Option 3a: Providing in the RTS a complete description of the algorithm and benchmarks to be used to assess and classify the inherent and residual risk profile of obliged entities.

Option 3b: Providing in the RTS a general description of the methodology and completing it with guidance from AMLA to all supervisors, to ensure a consistent application of the methodology.

A complete description of the algorithm in the RTS would achieve a high level of convergence as the detail of the methodology would be set out in directly applicable Union law. However, any changes to the methodology would have to take the form of an amendment to the legal text, which is complex and takes a long time. Since ML/TF risks are constantly evolving, this would create a risk that supervisors may be unable to reflect emerging risks in their risk assessment, which could hamper their ability to discharge their functions effectively. For this reason, it would be beneficial to ensure that the methodology is sufficiently flexible to be adjusted on a continuous basis, as necessary, in such a way that it can be adapted to existing ML/TF risks. This could be achieved if the methodology was described in the RTS in more general terms and complemented by guidance issued by AMLA, to ensure that it is applied consistently by all supervisors. Such an approach would allow flexibility to adjust the model. Finally, the reporting cost for the private sector is likely to be insignificant, as the full list of data points would be included in the RTS and would be unlikely to change frequently.

Based on the above, **Option 3b has been chosen as the preferred option** and the draft RTS on risk assessment and classification of the risk profile of obliged entities will provide a list of indicators

and a general description of the methodology that will need to be completed with further guidance from AMLA to all supervisors, to ensure a consistent application of the methodology.

Frequency of the assessment

Article 40(2) of Directive (EU) 2024/1640 provides that the RTS must set out the frequency at which risk profiles must be reviewed and adds that such frequency must take into account any major events or developments in the management and operations of the obliged entity, as well as the nature and size of the business. Regarding this point, the EBA considered three options.

Option 4a: set out the following frequencies of review:

- Once every year as the normal frequency;
- Once every two years as the frequency applying to obliged entities that are particularly small or only carry out certain activities justifying a reduced frequency;
- Ad hoc review, in a timely fashion, in the case of a major event or development in the management and operations of an obliged entity.

Option 4b: set out the following frequencies of review:

- At least once every year as the normal frequency;
- At least once every three years as the frequency applying to certain obliged entities that are particularly small or carry out only certain activities justifying a reduced frequency;
- Ad hoc review, in a timely fashion, in the case of a major event or development in the management and operations of an obliged entity.

Option 4c: set out the following frequencies of review:

- Once every year as the normal frequency;
- Once every two years as the frequency applying to certain obliged entities that are relatively small or carry out only certain moderately risky activities;
- Once every three years as the frequency applying to certain obliged entities that are particularly small or carry out only certain even lower-risk activities;
- Ad hoc review, in a timely fashion, in the case of a major event or development in the management and operations of an obliged entity.

The frequency of review should be proportionate to the nature and size of the obliged entities. Based on the experience of supervisors to date, to ensure that supervisors have an up-to-date understanding of the ML/TF risks to which the obliged entities under their supervision are exposed, the normal frequency at which risk profiles are reviewed should be once every year. In the case of certain entities, however, an annual data collection could be costly and have limited added value for supervisors, as the ML/TF risk score may not change significantly over time. This could particularly be the case for small obliged entities, and also for obliged entities that only carry out certain activities that justify a less frequent review and for obliged entities that are exposed to a

particularly low level of risk. The feedback received from the consultation confirmed that reviewing the profile of these obliged entities once every three years rather than annually would lead to a significant reduction in the cost borne by these obliged entities and by supervisors.

The EBA also considered whether collecting data and reviewing entities' risk profiles once every two years rather than once every three years for lower-risk obliged entities would be desirable. Feedback from supervisors suggests that the benefit to be gained from this approach is limited and that it would not significantly alter the understanding supervisors have of the level of ML/TF risk to which obliged entities are exposed, as obliged entities that are likely to benefit from this frequency are likely to be classified in the lower risk categories and would in any case be supervised with a limited intensity and at a limited frequency, in line with a risk-based approach. The feedback received from the public consultation confirmed that being reviewed once every three years rather than annually would significantly reduce the costs borne by firms subject to the reduced frequency.

Furthermore, splitting the group of lower risk entities into two groups, one of which would have its risk profile reviewed once every two years and the other with its risk profile reviewed once every three years appears to be of little benefit in comparison to the additional costs and layer of complexity it would introduce to the model. In any case, where major events or significant developments in the management and operations of an obliged entity are identified, supervisors should review its risk profile ad hoc, as rapid supervisory action may be warranted. The cost of these reviews for institutions or supervisors is unlikely to be significant as the occurrence of these types of events will likely be rare.

Based on the above, **Option 4b has been chosen as the preferred option** and the draft RTS on risk assessment and classification of the risk profile of obliged entities will set out the three following frequencies of review: (i) Once every year as the normal frequency; (ii) At least once every three years as the frequency applying to certain obliged entities that are particularly small or carry out only certain lower-risk activities; (iii) Ad hoc review, in a timely fashion, in the case of a major event or development in the management and operations of an obliged entity.

E. Conclusion

The draft RTS on risk assessment and classification of the risk profile of obliged entities will define the benchmarks and methodology for assessing and classifying the inherent and residual risk profile of obliged entities and set the frequency at which these risk profiles must be reviewed. For obliged entities and other stakeholders, the cost triggered by the draft RTS requirements are expected to be outweighed by the significant benefits in the medium to long term.

The EBA notes that a material portion of the costs will arise as a result of the move to a common risk assessment methodology based on provisions in AMLD6, which request that the draft RTS *'shall set out the benchmarks and a methodology for assessing and classifying the inherent and residual risk profile of obliged entities, as well as the frequency at which such risk profile shall be reviewed'*. The EBA's proposed approach nevertheless limits these costs as it reflects the proportionality principle and it is likely, in the short term, to bring benefits associated with the harmonisation of the data points that institutions have to provide and, in the medium to long term, to bring benefits

in terms of efficiency savings and reduced costs for reporting entities. It is also likely to make EU AML/CFT supervision more risk-based, targeted and effective. Overall, the impact assessment on the draft RTS suggests that the expected benefits for supervisors, obliged entities and other stakeholders are higher than the expected costs incurred.

4.2 Cost-benefit analysis / impact assessment – RTS under Article 12(7) AMLAR on the methodology for selecting credit institutions, financial institutions and groups of credit and financial institutions to be directly supervised by AMLA

A. Problem identification

A.1 Eligibility assessment

The AMLA shall treat as eligible financial sector entities that are operating in six or more Member States, either through an establishment or through the freedom to provide services. Operations under the freedom to provide services shall be measured, to assess their relevance.

Considering all operations under the freedom to provide services relevant, irrespective of their materiality, could have unintended consequences. For example, it could discourage the exercise of this freedom because being eligible incurs a fee, in accordance with Article 77 AMLAR. However, assessing the materiality of this type of operations is challenging, as feedback from competent authorities and the private sector suggests that data quantifying such operations is rarely recorded or available.

A.2 Risk assessment

AMLA shall put together a methodology to assess the ML/TF risk profiles of entities operating in six or more Member States. This methodology shall ensure a level playing field between all eligible obliged entities. Furthermore, it shall allow AMLA to assign a group-wide ML/TF risk score in cases where the obliged entity is a group.

A level playing field is not currently ensured, as supervisory approaches have not yet been harmonised, and competent authorities' ML/TF risk assessments are likely to differ as a result.

B. Policy objectives

The main objective of the draft RTS is to:

(i) identify the minimum activities that a credit institution or a financial institution has to carry out to be considered as operating under the freedom to provide services in a Member State that is different from the one where it is established. In this regard, to ensure an effective and proportionate selection process that keeps regulatory burden and cost to a necessary minimum, the draft RTS defines a materiality threshold beneath which operations under the free provision of services do not count towards an entity's presence in another Member State.

(ii) develop a risk assessment methodology that allows AMLA to assess and classify the inherent and residual risk profile of eligible credit institutions, financial institutions or groups of credit and financial institutions. To ensure an efficient approach and avoid duplication, this methodology should build on competent authorities' entity-level risk assessments under Article 40(2) AMLD6. For the first selection round, to obtain comparable entity-level risk assessment outcomes in a context where full harmonisation of AML/CFT supervisory practices is not yet assured, different rules will apply.

C. Baseline scenario

Regarding the assessment of the extent to which operations under the freedom to provide services are material, there is currently no structured reporting of data by obliged entities to their supervisors. Regarding the risk assessment that informs the selection of directly supervised entities, AML/CFT supervisory practices are not currently sufficiently harmonised to ensure comparable outcomes. In addition, the development of a group-wide methodology is challenging, considering the need to reflect in a proper way the overall ML/TF risk of the group, avoiding potential distortions of the final outcome.

D. Options considered

Measurement of the operations under the freedom to provide services

Article 12(7)(a) AMLAR requires AMLA to develop criteria to identify the "minimum activities" to be exercised under the freedom to provide services. Relying on notifications is unlikely to be a reliable indicator because it is common for credit or financial institutions to notify their intention to operate under the free provision of services to their financial supervisors without commencing activity in practice. It may also be the case that a credit or financial institution carries out activities under the freedom to provide services in a Member State, but these activities do not represent a substantial part of that entity's overall operation. Therefore, the EBA considers that a materiality threshold has to be identified. In this regard, the EBA has considered three different options.

Option 1a: Establishing a single threshold, to measure the number of customers

Option 1b: Establishing thresholds on customers and volumes of transactions, to be met together

Option 1c: Establishing thresholds on customers and volumes of transactions, to be met alternatively

Putting in place a threshold related to the number of customers under the freedom to provide services as the sole measure of materiality could eliminate from the selection entities and sectors with a small number of customers that perform a large number of activities in terms of their frequency and their value. Basing the materiality assessment on numbers of customers alone is therefore unlikely to be sufficient in all cases. For the same reason, putting in place a threshold for material volumes of transactions alone, or cumulative indicators of customer and volume thresholds, could eliminate potentially relevant cases from the selection. This suggests that setting

out metrics on customers and volumes of transactions and considering them as alternative measures would allow AMLA to capture all possible ways in which an entity can provide services across borders without an establishment in a material way.

As regards the values of the thresholds, the proposed approach is to set it based on the number of customers to 20 000, and volumes of transactions to EUR 50 000 000 per Member State, respectively. The proposed approach is expected to be proportionate to the size of an institution and its financial capacity. This is because being eligible for selection carries a fee, which may disproportionately affect smaller institutions, especially if they do not present high ML/TF risks.

Based on the above, **Option 1c has been chosen as the preferred option** and the draft RTS under Article 12(7) AMLAR, on the methodology for selecting credit institutions, financial institutions and groups of credit and financial institutions to be directly supervised by the AMLA will, for the purpose of measuring the operations under the freedom to provide services, establish thresholds on customers and volumes of transactions, to be met alternatively.

Calculation of the residual risk at entity level

Considering the synergies between the methodology for selection under Article 12(7) AMLAR and the methodology for risk assessment under Article 40(2) AMLD6, the former should build on the latter. However, the methodology under Article 40 AMLD6 envisages that competent authorities may apply manual adjustments to the control risk score based on qualitative assessments of an obliged entity's internal control system, to the extent that this information is available to supervisors. Considering the need to ensure the highest degree of comparability of the results of this risk assessment across Member States, and the current state of convergence of supervisory practices in the EU, three different options have been considered by the EBA.

Option 2a: Using the same methodology for the RTS under Article 12(7) and the RTS under Article 40(2) AMLD6 after the first selection round.

Option 2b: Developing two different methodologies, one for the RTS under Article 12(7) AMLAR and one for the RTS under Article 40(2) AMLD6.

Option 2c: Using the same methodology for the RTS under Article 12(7) AMLAR and for the RTS under Article 40(2) AMLD6, with limited differences to ensure maximum harmonisation and, for the first round of selection, adopting a divergent approach on the exercise of supervisory judgement for the determination of the control quality score.

Having a single methodology in place for Article 40(2) AMLD6 and Article 12(7)(b) AMLAR would reduce the reporting burden on obliged entities. However, choosing an option where two different methodologies have to be applied, one for the purpose of risk assessment under Article 40(2) AMLD6, and one for the purpose of selection, would require eligible obliged entities to provide data twice, using potentially different data points and timelines. This suggests that using the same methodology for the assessment of ML/TF risk under both Article 40 AMLD6 and Article 12 AMLAR would be preferable from an efficiency and effectiveness perspective. However, considering the

need to ensure full harmonisation and comparable outcomes, some differences are envisaged with regards to the calculation of inherent risk for the selection methodology.

Since the level of divergence of current AML/CFT supervisory practices across the EU is likely to lead to different assessments by supervisors of the quality of an entity's AML/CFT controls, the adoption of a divergent approach for the first round of selection that minimises the impact of supervisory judgement on the calculation of that score could lead to more harmonised and comparable outcomes after the first round.

Based on the above, **Option 2c has been chosen as the preferred option** and the draft RTS under Article 12(7) AMLAR on the methodology for selecting credit institutions, financial institutions and groups of credit and financial institutions to be directly supervised by AMLA will, for the calculation of the residual risk at entity level, use the same methodology for the RTS under Article 12(7) AMLAR and for the RTS under Article 40(2) AMLD6, with limited differences to ensure maximum harmonisation and, for the first round of selection, adopt a divergent approach on the exercise of supervisory judgement for the determination of the control quality score.

Risk assessment of groups

Article 12 AMLAR requires AMLA to assign a group-wide residual ML/TF risk score in case of groups of credit and financial institutions. Regarding the computation of this group score, the EBA considered two options.

Option 3a: Calculating the group score as a weighted average of all group entities' individual ML/TF risk scores

Option 3b: Assessing the whole group score as high ML/TF risk in cases where a certain number of the group's entities are high ML/TF risk

Calculating the group ML/TF risk score based on the weighted average of all entities' individual risk scores would consider the individual relevance of each of the group's entities compared to the whole group. On the other hand, setting a specific numerical threshold for treating the whole group as high risk in cases where a specific number of its entities have been assessed as high risk could exclude from the selection groups where the number of high-risk entities is inferior to the threshold set by the methodology, but where the high-risk entities significantly impact the group's operation. In terms of costs, aligning the selection with the level of operations (which can be correlated with greater financial strength) should also lead to selecting groups for which the high risk is coming from entities with greater financial strength.

Based on the above, **Option 3a has been chosen as the preferred option** and the draft RTS under Article 12(7) AMLAR on the methodology for selecting credit institutions, financial institutions and groups of credit and financial institutions to be directly supervised by AMLA will define the calculation of the group risk score as a weighted average of all group entities' ML/TF risk scores.

E. Conclusion

The draft RTS under Article 12(7) AMLAR on the methodology for selecting credit institutions, financial institutions and groups of credit and financial institutions to be directly supervised by AMLA will identify the minimum activities to be carried out by a credit institution or a financial institution for it to be considered as operating under the freedom to provide services in a Member State other than the one in which it is established. It will also include a risk assessment methodology that allows AMLA to assess and classify the inherent and residual risk profile of credit institutions, financial institutions and groups of credit and financial institutions based on the methodology that national supervisors will apply to assess entity-level ML/TF risk.

For obliged entities, the draft RTS are not expected to create significant costs. The main costs will be borne by competent authorities and stem to a large extent from underlying requirements in AMLAR, which state that the draft RTS must specify *'(a) the minimum activities to be carried out by a credit institution or a financial institution under the freedom to provide services, whether through infrastructure or remotely, for it to be considered as operating in a Member State other than that where it is established; (b) the methodology based on the benchmarks referred to in paragraphs 5 and 6 for classifying the inherent and residual risk profiles of credit institutions or financial institutions, or groups of credit institutions or financial institutions, as low, medium, substantial or high'*.

In the EBA's view, the draft RTS requirements are proportionate and limit costs where possible. They also bring benefits in relation to a consistent and harmonised approach to assessing entity-level ML/TF risk across the EU. Overall, therefore, the impact assessment on the draft RTS suggests that the expected benefits are higher than the incurred expected costs.

4.3 Cost-benefit analysis / impact assessment – RTS under Article 28(1) AMLR on Customer Due Diligence

A. Problem identification

Obliged entities in the EU have been required to apply CDD since the first AML directive came into force. Nevertheless, in line with the minimum harmonisation nature of the EU AML/CFT framework, the transposition of those requirements into the national legal systems of Member States was inconsistent. This created gaps in the EU's AML/CFT defences and additional costs for obliged entities that operated on a cross-border basis. Regulation (EU) 2024/1624 harmonises how CDD measures are conducted across EU Member States and across obliged entities within the EU.

B. Policy objectives

The general purpose of this mandate is to further harmonise the way due diligence measures are applied across the EU by specifying what information obliged entities shall collect to comply with their CDD, SDD and EDD requirements.

Compliance by obliged entities with the new CDD requirements introduced by AMLR will generate significant costs for obliged entities, according to private sector representatives that attended the EBA's roundtable in October 2024 or responded to its public consultation in 2025. Against this background, the EBA considered several policy options. The EBA's overall objective is to propose RTS that are risk-based and proportionate where possible, and conducive to effective outcomes while keeping associated compliance costs to a necessary minimum.

C. Baseline scenario

In the baseline scenario, obliged entities would comply with the requirements under the new EU AML framework pursuant to Chapter III of Regulation 2024/1624 without any further regulatory standards or guidance on how exactly they should comply.

D. Options considered

Degree of specification of Level 1 requirements

The aim of the mandate in Article 28(1) AMLR is to further harmonise the way customer due diligence measures are applied across the EU by setting out what information is necessary for the performance of customer due diligence. The EBA considered two options.

Option 1a: Assessing the Level 1 text to decide where specific provisions are needed to meet the policy objective, which is a harmonised, risk-based approach with effective outcomes. Level 1 requirements that are already sufficiently detailed would not be further specified.

Option 1b: Fostering maximum harmonisation by being as detailed and comprehensive as possible.

Under Option 1b, the draft RTS would set out specific requirements for every situation. This option would bring some benefits; for example it would maximise harmonisation, set clear regulatory expectations and make AML/CFT supervision – and possibly enforcement – easier by limiting the scope supervisors have to assess whether or not an obliged entity's approach is adequate. Nevertheless, by limiting the flexibility obliged entities have to adjust their controls, such an approach it is likely to make AML/CFT compliance less risk-based. It also means that obliged entities may be unable to respond effectively to situations that are not covered by the draft RTS.

By contrast, setting out a core set of rules and requirements that apply to all sectors and activities where necessary, as part of a maximum harmonisation framework within which obliged entities can identify the most suitable due diligence measures in light of the risks they have identified, will leave obliged entities room to adjust their CDD measures where this is warranted. Given the variety of obliged entities – in terms of size, business model and ML/TF risk exposure – to which these RTS will apply, this flexibility is likely to lead to more effective outcomes. This approach will also cater for situations unforeseen at this stage.

There are, nevertheless, a number of provisions in Regulation 2024/1624 that the draft RTS – taking into account the mandate in Article 28(1) of that Regulation – cannot further specify. These include, for example, the measures that obliged entities need to take to identify the beneficial owners, which are comprehensively laid out in Chapter IV of Regulation 2024/1624 on beneficial owner transparency. A similar point arises in relation to Articles 34(4)(e) and 34(4)(g) of Regulation 2024/1624, where the Level 1 text is sufficiently detailed, such that it would not require further clarification in the RTS.

Based on the above, **Option 1a has been chosen as the preferred option** and the draft RTS under Article 28(1) AMLR will further specify the Level 1 requirements only to the extent that this is necessary to achieve AMLR's policy objectives.

E. Review of responses from the public consultation

Out of the 170 responses the EBA received, 126 respondents came from the financial sector, including 38 responses from representatives of the banking sector.

The comparatively small proportion of responses from the non-financial sector means that benefits or costs incurred by unrepresented obliged entities may not be captured in this Impact Assessment.

1. Consultation results

Respondents expressed their support for the RTS. They welcomed the fact that the RTS contribute to harmonising customer due diligence requirements across the EU, that they take into consideration the proportionality principle, particularly the review cycle for low-risk entities, and that they introduce a transition period, especially as it relates to the requirement, in AMLR, to update CDD information for existing customers. Respondents described the EBA's approach to the transition period as pragmatic and said that it will ease implementation costs that would otherwise be borne by obliged entities. Respondents also welcomed other simplified measures identified in the RTS, such as allowing the simplification of measures for identifying and verifying the UBO in low risk situations.

Where respondents raised concerns, they highlighted the regulatory burden and costs of compliance associated with the RTS. Some considered that specific provisions exceeded AMLR requirements and highlighted concerns stemming from the use of restrictive or vague terminology or the narrow use of simplified measures in the RTS.

Respondents that expressed concerns regarding the application of risk-based approach noted that the RTS did not cater specifically for different types of obliged entities. Respondents also perceived certain requirements as too prescriptive. Requirements that could potentially exceed the requirements of AMLR included, for example, the requirement to collect both country and city of birth, the obligation for obliged entities to obtain and verify information on all nationalities held by customers, and the definition of complex structures. Other concerns included the limited flexibility for non-face-to-face verification apart from eIDAS, and the extent of information required for

understanding the ownership and control structure of a customer which is a legal entity, about customers' business associates and family members, and about senior managing officials. Lastly, respondents highlighted the use of undefined, potentially vague terms (e.g. 'legitimate reason'), restrictive use of sectoral simplified measures (in particular for pooled accounts and collective investment undertakings (CIUs)), and the limitations arising from some Member States' identity documents (e.g. due to some fields lacking information on place of birth and/or nationality).

2. Changes introduced by the EBA based on the public consultation responses

The EBA recognises that changes to institutions' CDD policies and procedures will have a significant impact on obliged entities. However, most of these costs will relate to provisions in AMLR itself, rather than to the clarifying measures set out in the EBA's draft RTS. Instead, the draft RTS will clarify the steps institutions will need to comply which should, over time, make regulatory expectations more transparent and, consequently, AML/CFT compliance more effective and efficient.

To further strengthen the risk-based approach, and keep costs of compliance to a necessary minimum where possible, the EBA revised and restructured the draft RTS on CDD after the public consultation concluded. These changes reinforce the application of the risk-based approach where possible.

The main changes the EBA introduced as a result of the private sector consultation and which have a positive impact on compliance costs for obliged entities include:

Proportionality and risk-based approach: The EBA introduced a new Article 1, which specifies that obliged entities must collect information and apply measures in line with a risk-based approach. It also ensures that both the scope of information and the measures applied across the RTS are proportionate to the ML/TF risk identified. Additionally, the EBA clarified that obliged entities are not required to collect all specified information in every case.

Information on 'city of birth': Since the operational costs of collecting the information on 'city of birth' are disproportionate to the value added for AML/CFT purposes, this requirement has been deleted. The EBA clarified, however, that it remains necessary to obtain at least the country of birth, which is sufficient to determine the place of birth, as required by AMLR, from the perspective of identification and risk mitigation.

Obtaining information on 'nationalities': The EBA understands that obtaining and verifying information on the nationalities of natural persons, particularly when persons hold multiple nationalities, imposes additional costs on obliged entities that may not be justified by a commensurate increase in the quality of ML/TF risk management. Therefore, the EBA has clarified that, where a person holds multiple nationalities and declares them in good faith, verifying one nationality is sufficient to meet AMLR's requirements.

Understanding the ownership and control structure of the customer: The EBA revised Article 11 of the draft RTS to address concerns that its initial proposal was too prescriptive. The new drafting clarifies the scope of intermediate entities in relation to which information should be collected, the

types of information to be collected and the circumstances under which it should be obtained, and makes the requirement more aligned with the ML/TF risk of the legal entity.

'Complex structures' (i.e. 'complex corporate structures' in the final RTS): The EBA revised the definition of complex structures in a way that does not capture a disproportionally high number of legal entities as 'complex structures' (for example through adjustment of the 'two or more layers'). In addition, the EBA also clarified that, in line with its original intent, legal entities which are identified by this definition as 'complex structures' do not automatically trigger enhanced due diligence measures. The terminology has been changed to 'complex corporate structures' to avoid any possible confusion with the 'excessively complex ownership structures' that are mentioned in Annex III of the AMLR as higher risk factors.

Equivalent information to be collected on senior managing officials (SMOs): Respondents indicated very high costs and significant difficulties in collecting the 'equivalent' information required for senior managing officials when they are identified as UBOs, especially as this information relates to the SMO's residential address. Since AMLR specifies that SMOs are not considered UBOs, the EBA clarified in the final RTS that the address of the registered office can be collected instead of the SMO's residential address.

Identification obligations for collective investment undertakings: In line with the principle of proportionality, the EBA extended the simplification provided by current Article 17 of the RTS to both low and standard risk cases (i.e. the possibility for CIUs to collect the information on final investors from the credit or financial institution that distributes its shares only upon request). This approach ensures proportionality and consistency, reflecting the CIU market structure where CIUs rely on CDD performed by AML obliged entities, thus avoiding extra costs and burdens.

Sectoral SDD measures for pooled accounts: The EBA accepted the request by respondents to explicitly exclude payment institutions (PIs) and e-money institutions (EMIs) from the application of Article 22 on pooled accounts, as in these cases the service is provided for the benefit of the payment service provider rather than final customers. Implementation of the provision could otherwise lead to de-risking of PIs and EMIs, higher fees and increased costs for consumers, potentially affecting competition.

Additional information on customers' 'family members and close associates': Respondents indicated certain data privacy-related limitations, as well as high costs in relation to collecting information on family members, persons known to be close associates or other close business partners and associates in the specific context of the enhanced due diligence measures. The EBA revised its initial approach to make the requirements less burdensome.

In addition, the EBA received a significant number of comments in relation to the interlink between the RTS on CDD and the eIDAS Regulation in relation to the non-face-to-face verification measures. Nearly all respondents indicated that obliged entities should not be requested to rely exclusively on eIDAS-compliant tools for verification of the identity of natural persons. The EBA agrees on this point with respondents and takes the view that remote solutions which are compliant with the EBA's Remote Customer Onboarding Guidelines should be considered as equal alternatives to eIDAS-compliant tools. However, given the EC's narrow interpretation of Article 22(6) AMLR, the

EBA was unable to introduce further flexibility than that already proposed in the consultation version in the specific article of the RTS on non-face-to-face verification measures.

E. Conclusion

The draft RTS under Article 28(1) AMLR will further harmonise the way due diligence measures are applied across the EU by harmonising the information to be collected by obliged entities to comply with their CDD, SDD and EDD requirements. For obliged entities and stakeholders (such as supervisors), the draft RTS requirements are not expected to trigger significant medium- to long-term costs as these requirements are linked to the AMLR requirements, and thus the costs incurred will be due to a great extent to the underlying related requirements set out in AMLR.

In addition, the EBA has made significant revisions to the RTS taking into account the information received through the public consultation on the proposed provisions aimed at reducing excessive costs linked to the implementation of the RTS.

Overall, the impact assessment on the draft RTS suggests that the expected benefits are higher than the expected costs incurred.

4.4 Cost-benefit analysis / impact assessment – RTS under Article 53(10) AMLD6 on pecuniary sanctions, administrative measures and periodic penalty payments

A. Problem identification

In 2020, the EBA published a report on the future AML/CFT framework in the EU to respond to a Call for Advice from the EC on the future AML/CFT framework[19]. In its response, the EBA underlined that NCAs' approaches to determining and imposing sanctions and other corrective measures for breaches of financial institutions' AML/CFT obligations were not consistent, and not always proportionate, effective or dissuasive. It stressed that harmonisation of the legal framework by means of directly applicable provisions in Union law was necessary to ensure an effective and robust approach.

Since then, the findings of fourth round of the implementation reviews performed by the EBA in 2023/2024[20] highlighted that while national supervisors assessed during that round had taken steps to strengthen their approach to enforcement, enforcement processes were not fully effective. Enforcement measures did not always create a sufficient deterrent response, and not all supervisors were using their enforcement powers in a proportionate way to achieve effective AML/CFT outcomes.

[19] Report on the future AML/CFT framework in the EU to respond to the EC's Call for Advice on defining the scope of application and the enacting terms of a regulation to be adopted in the field of preventing money laundering and terrorist financing.

[20] Report on NCAS' Approaches to the supervision of banks with respect to anti-money laundering and countering the financing of terrorism (Round 4 – 2023/24)

In parallel, the data reported by national supervisors to EuReCA, the EBA's AML/CFT database, suggest that supervisory approaches to enforcement continue to diverge. This means that the same breach by the same institution would be treated differently depending on where in the EU it occurs.

The mandate under Article 53(10) AMLD6 on pecuniary sanctions, administrative measures and PePPs aims to foster greater convergence of supervisors' approaches to enforcement and the imposition of administrative measures in the European Union. Moreover, it introduces PePPs as a new EU tool that aims to end an ongoing AML/CFT breach that is already subject to a specific administrative measure imposed by an AML/CFT supervisor. PePPs are currently used by only a few Members States in the EU.

B. Policy objectives

In Recital 126 AMLD6, RTS should ensure consistent harmonisation across the Union, and the EBA's policy objective is to harmonise approaches by AML/CFT supervisors in the EU when imposing sanctions, administrative measures and when introducing PePPs.

To achieve this, the mandate under Article 53(10) AMLD6 requests that AMLA set out, in the form of regulatory technical standards, (the draft RTS) (i) indicators to classify the level of gravity of breaches, (ii) criteria to be taken into account when setting the level of pecuniary sanctions or applying administrative measures, (iii) a methodology for the imposition of periodic penalty payments.

This mandate complements the provisions in Section 4 AMLD6 on pecuniary sanctions and administrative measures.

C. Baseline scenario

In the baseline scenario, supervisors would need to apply the provisions of AMLD6 in relation to pecuniary sanctions, administrative measures and PePPs embedded, respectively, in Articles 55, 56 and 57 AMLD6.

i. In line with the general provisions of Article 53 AMLD6, supervisors need to ensure that any pecuniary sanction imposed or administrative measure applied is effective, proportionate and dissuasive.

ii. Pursuant to Article 57 AMLD6, a periodic penalty payment shall be effective and proportionate and can be imposed until the obliged entity or person concerned complies with the relevant administrative measure, but not for longer than 12 months.

Without (i) common indicators defined to classify the level of gravity of breaches, (ii) criteria to be taken into account when setting the level of pecuniary sanctions or applying administrative measures, (iii) a methodology for the imposition of PePPs, this scenario is likely to lead to supervisors retaining divergent approaches to enforcement, which would make the EU's new approach less effective and would not meet the objectives of the AMLD6.

D. Options considered

Level of supervisory judgement

As mentioned above, the draft RTS will set out indicators for classifying the level of gravity of breaches, and criteria to be taken into account when setting the level of pecuniary sanctions or applying administrative measures. The indicators and criteria will be harmonised and inspired by existing EBA work on material weakness in the RTS on the central AML/CFT database[21] and the joint ESAs' report on the withdrawal of authorisation for serious AML/CFT breaches[22]. In the process of developing specific indicators and criteria, the EBA evaluated to what degree supervisory judgement should be exercised by NCAs. For this purpose, two options were considered.

Option 1a: Setting the indicators and criteria in the draft RTS with inspiration taken from existing EBA work on material weakness in the RTS on the central AML/CFT database[23] and the Joint ESAs Report on the withdrawal of authorisation for serious AML/CFT breaches[24] without any room for supervisory judgement.

Option 1b: Setting the indicators and criteria in the draft RTS with inspiration taken from existing EBA work on material weakness in the RTS on the central AML/CFT database[25] and the Joint ESAs Report on the withdrawal of authorisation for serious AML/CFT breaches[26] with room for supervisory judgement.

Leaving no room for supervisory judgement would provide for maximum convergence and meet the policy objective. However, it would not allow supervisors to take into account the specific context of the breach. This means that the resulting approach may not be proportionate to the breach or may lead to effective outcomes.

By contrast, Option 1b ensures a high level of convergence while providing for greater flexibility by enabling supervisors to consider the context of the breach. Taking into account the specific context of a breach allows a more in-depth analysis of the breach and the impact of the breach, and subsequently, enables supervisors to tailor the corrective or punitive measure to the specific situation. This makes a targeted and proportionate response possible and may ultimately lead to more effective enforcement.

The main stakeholders impacted by the choice of either option would be the competent authorities, with some impact on obliged entities.

i. As regards the competent authorities, the costs of either option would not be significantly different. In June 2025, the NCAs contributing to the work on the draft RTS on pecuniary

[21] Commission Delegated Regulation (EU) 2024/595, OJ L, 2024/595, 16.2.2024.

[22] ESAs 2022 23, 31 May 2022, Joint ESAs report.

[23] Commission Delegated Regulation (EU) 2024/595, OJ L, 2024/595, 16.2.2024.

[24] ESAs 2022 23, 31 May 2022, Joint ESAs report.

[25] Commission Delegated Regulation (EU) 2024/595, OJ L, 2024/595, 16.2.2024.

[26] ESAs 2022 23, 31 May 2022, Joint ESAs report.

sanctions, administrative measures and PePPs tested the functioning of the RTS indicators in practice by applying them to ongoing and past cases at national level. The results of this testing confirmed that the proposed approach as regards the indicator is correct, and that retaining room for supervisory judgement is important to ensure proportionate and effective outcomes.

ii. Separately, in response to the public consultation, some respondents were concerned that supervisors would have too much flexibility if the RTS provided room for supervisory judgement. To address this concern, clarifications and explanations were provided in the feedback table and amendments were made to Recital 3 and 4 of the draft RTS.

Based on the considerations above, **Option 1b remains the preferred option**. The draft RTS under Article 53(10), points (a) and (b), AMLD6 set the indicators and criteria in the draft RTS with inspiration taken from existing EBA work on material weakness in the RTS on the central AML/CFT database and the Joint ESAs Report on the withdrawal of authorisation for serious AML/CFT breaches, but with room for supervisory judgement. Following the public consultation, to address concerns expressed by some private sector stakeholders, the EBA introduced amendments to Recitals 3 and 4 of the draft RTS.

Periodic penalty payments

Pursuant to Article 53(10), point (c), AMLD6, the draft RTS will set out a methodology for the imposition of PePPs. The methodology proposed by the EBA was inspired by delegated and implementing acts adopted by the EC[27]. When developing the methodology for the imposition of PePPs, the EBA assessed the extent to which provisions of administrative law in the draft RTS should be harmonised, and considered two options.

Option 1a: Setting out a granular set of provisions of administrative law by minimising room for the application of national provisions of administrative law.

Option 1b: Competent authorities to apply their national provisions of administrative law when imposing PePPs.

Leaving little or no room for the application of national provisions of administrative law would provide for maximum convergence and would be in line with the policy objective. It would not allow supervisors to take into account longstanding specific jurisprudence in the area of administrative law and would require them to apply different provisions of administrative law when enforcing PePPs compared to other enforcement measures. This could have unintended consequences and mean that supervisors might avoid using PePPs as defined by AMLD6, as their imposition is a choice and not a duty of the supervisor.

[27] For instance: Commission Delegated Regulation (EU) No 667/2014, OJ L 179, 19.6.2014, pp. 31–35 as amended, Commission Implementing Regulation (EU) No 646/2012 of 16 July 2012, OJ L 187, 17.7.2012, pp. 29–35.

On the other hand, leaving room for the application of national provisions of administrative law when imposing PePPs would ensure convergence, while providing more flexibility when imposing PePPs.

The main stakeholders impacted by the choice of either option would be competent authorities.

The costs would not change significantly with either option; potentially, costs could be lower by focusing only on some aspects of the methodology for the imposition of PePP to be included into the draft RTS, as this would not require a complete review and amendment of national provisions of administrative law in 27 Member States for the purpose of the imposition of PePPs.

Based on the above, **Option 1b has been chosen as the preferred option** and the draft RTS under Article 53(10), point (c), and AMLD6 set a methodology for PePPs in the draft RTS by allowing supervisors to apply procedures stipulated by national administrative law.

The extent of provisions of substantive law concerning the methodology included into the draft RTS mirrors the general agreement that could be reached. The future application of these RTS, once adopted, will show whether and to what extent further changes and amendments could be even more beneficial for a harmonised approach by AML/CFT supervisors.

E. Conclusion

The draft RTS under Article 53(10) AMLD6 on pecuniary sanctions, administrative measures and PePPs set out indicators to classify the level of gravity of breaches, criteria to be taken into account when setting the level of pecuniary sanctions or applying administrative measures, and a methodology for the imposition of PePPs. This supports the adoption of more convergent approaches by EU AML/CFT supervisors to imposing sanctions, administrative measures and PePPs.

The main stakeholders impacted in terms of costs by the draft RTS would be the competent authorities, but some of these costs are associated with underlying legal requirement in AMLD6. The testing performed by NCAs taking part in the workstream confirmed the approach followed in the draft RTS as regards the indicators and opportunities to exercise supervisory judgement. Overall, taking into account the EBA's preference for a proportionate approach where possible, while ensuring consistent and effective comparable outcomes, the impact assessment on the draft RTS suggests that the expected benefits are higher than the incurred expected costs.

4.5 Overview of questions for consultation

RTS under Article 40(2) AMLD6

Question 1

Do you have any comments on the approach proposed by the EBA for assessing and classifying the risk profile of obliged entities?

Question 2

Do you agree with the proposed relationship between inherent risk and residual risk, whereby residual risk can be lower, but never higher, than inherent risk? Would you favour another approach instead, whereby the obliged entity's residual risk score can be worse than its inherent risk score? If so, please set out your rationale and provide evidence of the impact the EBA's proposal would have.

Question 3

Do you have any comments on the proposed list of data points in Annex I to this Consultation Paper? Specifically:

- What will be the impact, in terms of cost, for credit and financial institutions to provide this new set of data in the short, medium and long term?
- Among the data points listed in the Annex I to this consultation paper, which are those that are not currently available to most credit and financial institutions?
- To what extent could the data points listed in Annex I to this Consultation Paper be provided by the non-financial sector?

Please provide evidence where possible.

Question 4

Do you have any comments on the proposed frequency at which risk profiles would be reviewed (once per year for the normal frequency and once every three years for the reduced frequency)? What would be the difference in the cost of compliance between the normal and reduced frequency? Please provide evidence.

Question 5

Do you agree with the proposed criteria for the application of the reduced frequency? What alternative criteria would you propose? Please provide evidence.

Question 6

When assessing the geographical risks to which obliged entities are exposed, should cross-border transactions linked with EEA jurisdictions be assessed differently than transactions linked with third countries? Please set out your rationale and provide evidence.

RTS under Article 12(7) AMLAR

Question 1

Do you agree with the thresholds provided in Article 1 of the draft RTS and their value?
If you do not agree, which thresholds to assess the materiality of the activities exercised under the freedom to provide services should the EBA propose instead? Please explain your rationale and provide evidence of the impact the EBA's proposal and your proposal would have.

Question 2

What is your view on the possibility of lowering the value of the thresholds that are set in Article 1 of the draft RTS? What would be the possible impact of doing so? Please provide evidence.

Question 3

Do you agree on having a single threshold on the number of customers, irrespective of whether they are retail or institutional customers? Alternatively, do you think a distinction should be made between these two categories? Please explain the rationale and provide evidence to support your view.

Question 4

Do you agree that the methodology for selection provided in these RTS builds on the methodology laid down in the RTS under Article 40(2)? If you do not agree, please provide your rationale and evidence of the impact the EBA's proposal and your proposal would have.

Question 5

Do you agree that the selection methodology should not allow the adjustment of the inherent risk score provided in Article 2 of draft under Article 40(2) AMLD6? If you do not agree, please provide the rationale and evidence of the impact the EBA's proposal would have.

Question 6

Do you agree with the methodology for the calculation of the group-wide score that is laid down in Article 5 of the RTS? If you do not agree, please provide the rationale for it and provide evidence of the impact the EBA's proposal and your proposal would have.

Question 7

Do you have any concerns about the identification of the group-wide perimeter? Please provide the rationale and the evidence to support your view on this.

Question 8

Do you agree to give the same consideration to the parent company and the other entities of the group for the determination of the group-wide risk profile? Do you agree this would reliably assess the group-wide controls' effectiveness, even if the parent company has an activity with low relevance compared to the other entities?

Question 9

Do you agree with the transitional rules set out in Article 6 of this RTS? If you don't, please provide the rationale for this and provide evidence of the impact the EBA's proposal and your proposal would have.

RTS under Article 28(1) AMLR

Question 1

Do you agree with the proposals as set out in Section 1 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Question 2

Do you have any comments regarding Article 6 on the verification of the customer in a non-face-to-face context? Do you think that the remote solutions, as described under Article 6 paragraphs 2-6, would provide the same level of protection against identity fraud as the electronic identification means described under Article 6 paragraph 1 (i.e. eIDAS-compliant solutions)? Do you think that the use of such remote solutions should be considered only temporary, until such time as eIDAS-compliant solutions are made available? Please explain your reasoning.

Question 3

Do you have any comments regarding Article 8 on virtual IBANS? If so, please explain your reasoning.

Question 4

Do you agree with the proposals as set out in Section 2 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Question 5

Do you agree with the proposals as set out in Section 3 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Question 6

Do you agree with the proposals as set out in Section 4 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Question 7

What are the specific sectors or financial products or services which, because they are associated with lower ML/TF risks, should benefit from specific sectoral simplified due diligence measures to be explicitly spelled out under Section 4 of the daft RTS? Please explain your rationale and provide evidence.

Question 8

Do you agree with the proposals as set out in Section 5 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Question 9

Do you agree with the proposals as set out in Section 6 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Question 10

Do you agree with the proposals as set out in Section 7 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Question 11

Do you agree with the proposals as set out in Section 8 of the draft RTS (and in their linked Annex I)? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Draft RTS under Article 53(10) AMLD6 on pecuniary sanctions, administrative measures and periodic penalty payments

Question1

Do you any have comments or suggestions regarding the proposed list of indicators for classifying the level of gravity of breaches sets out in Article 1 of the draft RTS? If so, please explain your reasoning.

Question 2

Do you have any comments or suggestions on the proposed classification of the level of gravity of breaches sets out in Article 2 of the draft RTS? If so, please explain your reasoning.

Question 3

Do you have any comments or suggestions regarding the proposed list of criteria to be taken into account when setting up the level of pecuniary sanctions of Article 4 of the draft RTS? If so, please explain your reasoning.

Question 4

Do you have any comments or suggestions to add regarding what needs to be taken into account as regards the financial strength of the legal or natural person held responsible (Article 4(5) and Article 4(6) of the draft RTS)? If so, please explain.

Question 5

Do you have any comments or suggestions on the proposed criteria to be taken into account by a supervisor when applying the administrative measures listed under these draft RTS, and in particular when the supervisor intends to:

- restrict or limit the business, operations or network of institutions comprising the obliged entity, or to require the divestment of activities as referred to in Article 56(2)(e) of Directive (EU) 2024/1640?
- withdrawal or suspension of an authorisation as referred to in Article 56(2)(f) of Directive (EU) 2024/1640?
- require changes in governance structure as referred to in Article 56(2)(g) of Directive (EU) 2024/1640?

Question 6

Which of these indicators and criteria could also apply to the non-financial sector? Which ones should not apply? Please explain your reasoning.

Question 7

Do you think that the indicators and criteria set out in the draft RTS should be more detailed as regards the natural persons that are not themselves obliged entities and in particular as regards the senior management as defined in AMLR? If so, please provide your suggestions.

Question 8

Do you think that the draft RTS should be more granular and develop more specific rules on factors and on the calculation of the amount of the PePPs and, if yes, which factors should be included in the EU legislation and why?

Question 9

Do you think that the draft RTS should create a more harmonised set of administrative rules for the imposition of periodic penalty payments and, if yes, which provisions of administrative rules would you prefer to be included in EU legislation compared to national legislation and why?

4.6 Feedback on the public consultation

The EBA publicly consulted on a version of the draft RTS contained in the consultation paper. The consultation period lasted for 3 months and ended on 6 June 2025. The EBA received 170 responses, of which 108 were published on the EBA website.

This section presents a summary of the key points arising from the consultation responses. The feedback table in the following section provides further details on the comments received from the analysis performed by the EBA, and the actions taken to address the comments if necessary.

The views of the Banking Stakeholder Group can be consulted here. The contents of the document referred to via the hyperlink shall be deemed to be repeated and incorporated herein by reference.

RTS under Article 40(2) AMLD6 – Summary of the key issues and the EBA's response

Respondents welcomed the move towards a more harmonised approach to the assessment of the level of ML/TF risks to which obliged entities are exposed within the Union. The use of a common methodology based on a single set of indicators and benchmarks was seen as fostering a level playing field within the Union. Respondents also considered that this would help reduce regulatory arbitrage, facilitate cross-border operations and help make the EU's approach to AML/CFT supervision more targeted and effective. The application of a reduced frequency of review to obliged entities that are particularly small or that carry out certain types of low-risk activities was regarded as a sensible measure which should alleviate the regulatory burden placed on these types of entities. Where respondents raised concerns, these related to the number of proposed data points, the extent to which the methodology was described in the legal text and the frequency at which the risk profile of all obliged entities would be reviewed.

1. **Number of data points**

Several respondents were concerned that the proposed number of data points may be too high. They also observed that several of the proposed data points were unclear or not readily available in all Member States. Institutions would need to adapt their IT systems or perform complex data gathering exercises to be able to report. This could induce significant short-term costs.

As reflected in the impact assessment (Section 4.1), the EBA recognises that adapting to a new framework will entail initial set-up costs for most institutions. At the same time, the EBA considers that these initial costs will be outweighed in the medium and long term by the benefits of having a harmonised approach at Union level.

To address respondents' concerns, to make the proposed risk assessment more effective and reduce the reporting burden on institutions where possible:

- the EBA clarified in the draft legal text which data points should apply to which sector. It also prepared an interpretive note that will accompany the RTS. These changes are designed to ensure that each data point will be interpreted unequivocally by institutions and their supervisors.

- the EBA assessed the importance of each data point using feedback from the public consultation and an NCA-led exercise with data from over 100 financial institutions. It reduced the number of proposed data points by 15% as a result. This means that the final number of data points that an average institution would typically be required to report will average 100-150 data points for most institutions. This number is significantly lower than current reporting standards in most Member States.

2. The level of detail contained in the legal text

Some respondents noted that aspects of the methodology were not set out in the draft RTS. They said that this meant that the scoring system was not fully transparent.

ML/TF risks emerge and evolve. For this reason, the methodology needs to adapt. Setting all parameters out in the RTS would require amendments to the RTS every time a new risk emerges or existing risks change. Since amending legislation takes time, the ongoing pertinence of entity-level risk assessments would not be ensured. To address this, and in line with the approach adopted by prudential supervisors, several aspects of the methodology are set out in a separate document that AMLA will manage instead. However, to ensure that institutions can anticipate reporting requirements and take the steps necessary to supply the requested information in good time, the EBA considers that data points should be stable over time and included in the legal text.

3. Frequency of review of the risk profile of obliged entities

Respondents welcomed that the EBA had proposed adjustments to the frequency at which the risk profile of obliged entities should be reviewed in line with a risk-based approach, but several respondents questioned whether alternative approaches to determining this frequency would yield more proportionate outcomes. For example, some respondents suggested that the default frequency should be once every three years for all institutions instead of once every year. They suggested that firms' business models were sufficiently stable overall to justify a less frequent assessment. The provisions on major events or developments in the management and operations of obliged entities could act as a safeguard, allowing supervisors to perform an ad hoc reassessment when needed.

Supervisors need to be able to keep track of the evolution of ML/TF risks within institutions, to be able to spot trends and tendencies within the market. Competent authorities were concerned that this may not be possible if risk profiles were reviewed only once every three years. Provisions on major events or developments in the management and operations of obliged entities do not replace the periodic assessment conducted by supervisors but instead allow supervisors to rapidly update their understanding of associated risks and react accordingly if needed, without waiting for the next assessment cycle. For this reason, and in line with the strong steer from competent authorities, the EBA retained the approach set out in the consultation document.

In taking its decision, the EBA also considered the use of alternative ways to determine which institutions could benefit from reduced assessment cycles. For example, the EBA assessed, in close collaboration with competent authorities, whether basing the criteria on existing notions such as

the concept of 'small and non-complex institutions' included in Regulation (EU) No 575/2013, or including alternative criteria such as the stability of the business or the number of customers could lead to a more proportionate approach without jeopardising the overall reliability of the risk assessment. The EBA ultimately concluded that the proposed approach was conducive to the most proportionate and robust outcomes.

RTS under Article 12(7) AMLAR – Summary of the key issues and the EBA's response

Overall, respondents welcomed efforts made to create a unified approach, which builds on the risk assessment at national level. Respondents believed that this approach was sensible and would help to create a consistent framework for identifying and classifying ML/TF risk at Union level. They also felt that it would help reduce the reporting burden on obliged entities by using one single set of data points to perform both assessments, under Article 40(2) AMLD6 and Article 12(7) AMLAR.

Where respondents raised concerns, these related to the timeline and the value of the material thresholds. Some respondents also found it unclear how the two draft RTS would interact.

1. **Timeline**

Several respondents suggested that performing the assessment in 2027 may be too ambitious, because this would require firms to report data for the year 2026. They said this would leave them too little time to prepare.

The EBA recognises that the timeline may be challenging for the private sector. At the same time, the date by which the assessment must be performed is set out in Article 13(4) AMLAR and cannot be amended by the draft RTS.

To address the concerns raised by respondents, the EBA proposed to exclude a small number of data points from the first assessment process that are important but may be challenging or costly to obtain at short notice.

2. **Interaction between the two draft RTS**

Some respondents found it unclear how the two draft RTS would interact. Some of them believed that both methodologies would be applied in isolation, leading to two distinct data collection exercises and using two separate scoring systems.

The EBA clarifies that the assessment performed for the purpose of the selection process under Article 12(7) AMLAR will not be performed in addition to the assessment under Article 40(2) AMLD6 but will instead build on it (Figure 2). This is because, according to the EBA's proposals and in line with AMLAR, the outcome of the risk assessment under Article 40(2) will feed into the assessment under Article 12(7). Therefore, a single reporting channel and scoring system can be used to perform both assessments.

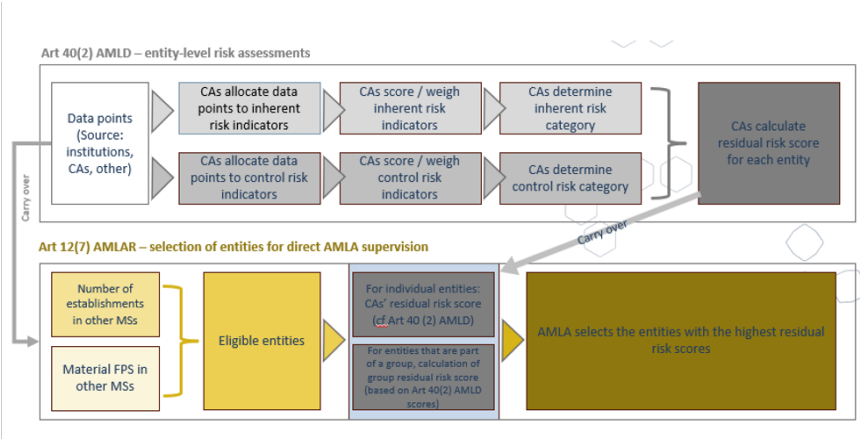

Figure 2: Interaction between the risk assessments under Articles 40(2) AMLD6 and 12(7) AMLAR

3. Value of the materiality thresholds

There was no consensus among respondents on the proposed values of the proposed thresholds for determining the materiality of an institution's free provision of services. Some respondents suggested that the thresholds were too high and would only capture entities within large groups. Others claimed that they were too low and would be exceeded by a significant number of entities in certain sectors (such as the crypto and asset management sectors). Respondents did not provide evidence to support their statements.

The EBA is mindful of the impact these thresholds will have, since being eligible for direct supervision by AMLA carried a fee. For this reason, the EBA reached out to competent authorities and EU trade associations representing different sectors or groups of national financial sector trade associations to obtain further information.

Most trade associations declined to provide further information. They said it was the role of national supervisors to inform the EBA of the extent to which their sector's cross-border operations were material. Since data provided by competent authorities confirmed the proposed materiality thresholds, the EBA did not bring any changes to the draft legal text.

RTS under Article 28(1) AMLR – Summary of key issues and the EBA's response

Respondents supported the RTS proposed by the EBA to further harmonise the way due diligence measures are applied across the EU. They considered that the EBA's approach was proportionate and pragmatic. They also welcomed the introduction of a transition period in relation to updating CDD information for existing customers. Where respondents raised concerns, these generally related to the balance between a rules-based and a more risk-based approach, the interpretation of wider provisions and terms in the Level 1 text, and the application of SDD. A significant number of submissions were also received on the draft non-face-to-face verification measures.

The risk-based approach

Many respondents remarked that the risk-based approach ('RBA') should be central to the application of customer due diligence measures. They wanted the EBA to ensure that the RTS will preserve the risk-based approach, which is tailored to different types of obliged entities and to the different level of ML/TF risks. They also considered that provisions of the RTS should not go beyond what the underlying AML Regulation requires. They stated that, otherwise, the RTS would create unnecessary administrative burden and would unnecessarily increase the cost of compliance.

The EBA's work on these RTS was guided by the principles of a proportionate, risk-based approach that focuses on effective outcomes. For example, the proposed draft RTS remain silent where sufficient detail is provided in the AMLR and sets out options institutions can consider when deciding on the most effective and proportionate way to address specific compliance challenges, while ensuring compliance with AMLR. At the same time, the draft RTS cannot propose actions that would put institutions that applied them in breach of their obligations under AMLR. This means that, at times, provisions in AMLR, or the EC's interpretation of those provisions, limited the EBA's ability to apply a fully risk-based approach.

To further clarify where a risk-based approach is possible, the EBA brought several changes to the draft RTS. It also introduced a new article that specifies that provisions in the draft RTS are to be applied in a risk-sensitive way.

Definition of key concepts and terms

Several respondents raised questions on the interpretation of concepts and provisions of AMLR. Examples of such concepts include:

i. The term 'transaction being conducted on behalf of or for the benefit of natural persons other than the customer' (Article 20(1)(h) AMLR).
ii. 'Information to be collected on senior managing officials when they are identified as [ultimate beneficial owners] (Article 22(2), subparagraph 2, AMLR)', which may, according to respondents to the EBA's public consultation, be in conflict with data privacy requirements.

The EBA agrees that some cross-cutting concepts and terms used in the AMLR might benefit from further clarification. Clarifying these concepts and terms could be conducive to the consistent interpretation and application of the Level 1 text. However the EBA mandate under Article 28(1) AMLR does not extend to the interpretation of those terms.

It will fall to AMLA, in consultation with the EC, to consider whether further work on those concepts and terms would be warranted.

Simplified due diligence and the cost of compliance

Some respondents were concerned about the possible regulatory burden and cost of compliance associated with the RTS. They also inquired whether other financial products and services could benefit from specific sectoral simplified measures.

While keeping in mind the limitations of the scope of the mandate under Article 28(1), the EBA amended several provisions to reduce regulatory burden and cost of compliance. For example:

- In relation to the identification of legal entities: the EBA clarified in the draft RTS that it was not mandatory to obtain the registration number, tax identification number and LEI simultaneously; obtaining any one of these identifiers is sufficient. Additionally, the final RTS provide that information on the source of funds does not need to be obtained as a general requirement, but only when necessary.

- In relation to the CIUs: the EBA extended the simplification already provided (i.e. the possibility for CIUs to collect the information on final investors from the credit or financial institution that distributes its shares only upon request) to both low and standard risk cases. This approach ensures proportionality and consistency, reflecting the CIU market structure where CIUs rely on CDD performed by other obliged entities, thus avoiding extra costs and burdens.

- In relation to pooled accounts: the EBA excluded PIs and EMIs from the application of Article 20 of the RTS on pooled accounts, as in these cases the service is provided for the benefit of the payment service provider rather than final customers. Implementation of the provision by the credit institutions opening the account could otherwise lead to de-risking of PIs and EMIs, higher fees and increased costs for consumers, potentially affecting competition.

- Going forwards, AMLA, in consultation with the EC, may wish to consider defining additional simplified measures for the financial and non-financial sectors, based on the EU-wide Supranational Risk Assessment and in consultation with the network of experts from Member States.

Verification of identity on a non-face-to-face basis and the role of non-eIDAS certified tools

The majority of respondents to the public consultation requested that the draft RTS do not distinguish between non-eIDAS solutions and eIDAS solutions for the purpose of verifying the identity of a customer remotely. They considered that the cost of not doing so was high and could have unintended consequences, such as an increase in fraud or unwarranted de-risking. Furthermore, the use of an eIDAS-compliant identification solution by EU customers is a choice rather than a legal requirement and could not be made mandatory by way of draft RTS.

Respondents indicated that the benefits of using other tools which meet the requirements of Article 7(3) of the RTS, would include:

- ensuring that non-EU residents or non-EU customers are not excluded from financial services provided by EU-based obliged entities;
- enhancing financial inclusion and promoting innovation in financial services;
- making the EU financial system more resilient to fraud attacks;
- promoting the principle of technological neutrality;
- limiting the cost of compliance as the provisions, as drafted, would mean that obliged entities equip themselves with two tools for verification purposes: one that is eIDAS-compliant and another that is not.

As indicated in the Impact Assessment, the EBA considers that the same objective, i.e. the robust mitigation of ML/TF risk where customers are not physically present, could be achieved by giving institutions a choice of tools they will deploy for that purpose. The advantage of a more flexible approach would be a reduction in the cost of compliance, as institutions could opt for the approach that best meets their operational needs and ML/TF risk exposure. It would also address concerns about possible unintended consequences, such as the risk of financial exclusion of vulnerable customers who may not have access to eIDAS-compliant IDs, lack of competition or an increase in the risk of identity fraud. The EBA Remote Customer Onboarding Guidelines contain examples of the type of solutions institutions could use. However, in line with the EC's reading of AMLR, eIDAS solutions are legally required in this context, which means that the EBA has not amended the draft RTS on this point.

Draft RTS under Article 53(10) AMLD6 on pecuniary sanctions, administrative measures and periodic penalty payments

Summary of key issues and the EBA's response

Respondents supported the objective of a harmonised EU enforcement regime, welcoming more clarity, consistency and proportionality. They also supported the classification of the gravity of breaches in different categories and the proposed structured approach to setting fines, considering cooperation, remediation, intent, benefit from the breach, harm, and an institution's past record of breaches.

Where respondents raised concerns, these were mainly related to the indicators and criteria set out in the draft RTS, ongoing differences in Member States' approaches to enforcement and the potential interaction between the principles of non-self-incrimination and lack of cooperation set out in the proposed RTS.

The coherence of such an approach has also been confirmed by a preliminary testing of the indicators performed by the dedicated workstream on ongoing and past enforcement cases at national level.

1) **Indicators and criteria**

Respondents welcomed the convergence provided by the draft RTS, but several underlined that the lists of indicators and criteria specified by this RTS were non-exhaustive. They felt that this granted too much discretion to supervisors and could lead to inconsistent enforcement. Some respondents suggested either expanding the list or ensure that any additional factors are transparently communicated to obliged entities. Respondents further highlighted the need for transparency in how the indicators and criteria will be applied. Some suggested that AMLA should develop or request that NCAs develop internal sanctioning policies or guidelines. In their view, this would ensure consistency and build trust in the rulebook. Finally, several respondents suggested that the use of the same facts to classify a breach and determine the amount of the penalty could be problematic.

To support the consistent application of the new enforcement framework, the EBA:

- amended Recital 3. In line with AMLD6, supervisors should take into account ''all relevant circumstances when determining the type and level of pecuniary sanctions or administrative measures. Therefore, the indicators and criteria listed in the draft RTS should not be considered exhaustive, as other relevant circumstances and the supervisory judgement of the Authority must also be taken into account. To reduce inconsistencies in assessments, the EBA has clarified that any additional indicators or criteria identified by the supervisor should be specific to allow for proper evaluation and justification. Moreover, they should be part of the supervisor's overall assessment of indicators and criteria listed in the draft RTS. This is to ensure convergence and consistency across Member States while at the same time enabling supervisors to take into account the specific context in which the breach has occurred. Supervisors should ensure that their supervisory judgement is coherent and consistent, with comparable outcomes.
- amended some indicators and criteria to further clarify their interpretation. While the EC's Call for Advice to the EBA did not extend to the drafting of sanctioning policies or guidelines, AMLA may consider doing so.
- Regarding the use of the same facts to classify a breach or determine a penalty that is proportionate to the breach, the EBA is of the view that in accordance with provisions of Art 53(6) AMLD6 and supervisory practice, some circumstances such as the conduct of the person held responsible can be considered, albeit under a different perspective, both as an indicator to classify the gravity of the breach and as a criterion for setting the level of pecuniary sanctions. It should be noted that this does not apply to the majority of the indicators and criteria provided.

2) **Differences between criminal and administrative enforcement in EU countries**

Some respondents noted differences in how AML/CFT breaches are treated across Member States. In some Member States, certain breaches face criminal enforcement but will be subject only to administrative enforcement in other Member States. They consider that such divergence may lead to the unequal treatment of obliged entities, depending on their jurisdiction and would welcome a more harmonised approach in the draft RTS.

The EBA supports harmonisation in enforcement, as set out in its response to the EC's 2020 Call for Advice on the future AML/CFT framework. However, aligning criminal and administrative powers is outside of the mandate of the RTS.

3) **Non-cooperation as an aggravating criterion to increase the level of a pecuniary sanction**

Some respondents expressed concerns about penalising non-cooperation when an entity may fail to cooperate to protect its rights in parallel criminal proceedings. They suggested that this criterion be deleted.

Article 53(6) AMLD6 provides that, 'when determining the type and level of pecuniary sanctions or administrative measures, supervisors shall take into account: […] '(*g) the level of cooperation of the natural or legal person held responsible with the competent authority'*. The draft RTS refer to the level of cooperation supervisors may reasonably expect, in compliance with the fundamental principle of non-self-incrimination that applies to all enforcement proceedings and does not have to be set out specifically in the draft RTS.

Summary of responses to the consultation and the EBA's analysis

Responses to questions relating to the RTS on the assessment of the inherent and residual risk profile of obliged entities (Article 40(2) AMLD6)

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Articles 2 to 4 Transparency of the scoring system	A number of respondents noted the absence of information on the values of the thresholds that will be used to score the indicators and on the weights that will be assigned to each of them. These respondents claim that this prevents obliged entities from evaluating the validity and proportionality of the methodology.	Some technical details of the methodology (including the scoring thresholds and weights) are not included in the draft RTS. This is because the model needs to be sufficiently flexible, to allow AMLA to adjust it on an ongoing basis, based on the evolution of ML/TF risks and business models, without having to amend the RTS (which is a long and cumbersome process. At the same time, it is key that the private sector has access to the data points that will be used as a basis for the assessment as early as possible, to be able to anticipate future reporting requirements and prepare accordingly.	None.

		This justifies their inclusion in the legal text.	
Article 3 Manual adjustment of control quality scores based on professional judgement	Some respondents were concerned that the possibility of manually adjusting the control quality score based on professional judgement or an external auditor's assessment could introduce biases to the detriment of entities that are subject to more frequent and intensive scrutiny. Respondents were also concerned that inconsistencies could result from divergent approaches by different supervisors.	While assessing the quality of controls based purely on an automated scoring system is necessary for certain entities that are supervised at a very low intensity, supervisory assessments (especially on-site inspections) and external auditors' assessments will generally provide supervisors with much more accurate information on the quality of the AML/CFT controls put in place by an entity. Therefore, where such assessments are available, they should prevail over the automated score. It is, however, key that supervisory assessments are performed in a consistent manner across the Union. It will be AMLA's role to ensure that supervision is conducted in a harmonised manner across the different Member States.	None.
Article 5 Normal frequency of review	Several respondents claimed that the default frequency of review should be reduced. They suggested that the default frequency should be once every three years. These respondents argued that ML/TF risk profiles are usually quite stable over time. If a significant development	It is key that supervisors can keep track of the evolution of ML/TF risks. Currently, ML/TF assessments are performed on an annual basis in most Member States. The experience of	None.

	occurs, they also claim that the provisions on major events would allow supervisors to conduct an ad hoc review.	national supervisors suggests that changes in the risk profile of obliged entities may occur sufficiently often to justify a general principle of reviewing such risk profiles on a yearly basis. Furthermore, the provisions on major events or developments in the management and operations of obliged entities are not aimed at replacing the periodic assessment conducted by supervisors. The intention is for supervisors to conduct a targeted reassessment in a short period of time if a significant event occurs, so that they can update their understanding of the risks and react accordingly if needed, without having to wait for the next assessment cycle. Such ad hoc reassessment also presupposes that supervisors are aware of the occurrence of the major event, which may not always be the case.	
Article 5 Reduced frequency of review – Number of FTEs and size criteria	There were divergent views regarding the inclusion of five FTEs as a component of the criteria for reduced frequency of review with arguments either to increase or remove this criterion. Some respondents argued that a smaller number of FTEs does not necessarily mean lower risk. The argument to increase mainly came from smaller entities advocating a carve-out ranging from 10 FTEs to 50 FTEs or using a different approach (for instance by building upon	The criterion was introduced to ensure that the requirements applicable to very small firms are not overly burdensome. Should the threshold be raised, certain entities for which an annual frequency would be warranted as a result of their	None.

the notion of small and non-complex institutions within the meaning of Regulation (EU) No 575/2013).

A number of respondents also suggested the inclusion of additional size criteria, such as:

- A stable nature of nature of business activities;
- Number of customers;
- Volume of transactions;
- Operation in a low-risk sector as identified in the national risk assessment;
- The demonstration of robust AML/CFT controls.

However, none of them provided specific suggestions as to how these criteria should be interpreted or assessed.

high exposure to ML/TF risk might be captured and unduly subjected to a reduced frequency.

The notion of small and non-complex institutions applies to institutions that may be significantly bigger than those whose staff represents 5 FTEs or fewer. Therefore, using this option is not a credible option.

Lastly, the inclusion of additional size criteria appears difficult to implement. Regarding the number of customers and value of transactions, in the absence of available data on the values that would be associated with different types and sizes of institutions, these criteria would be difficult to calibrate. Regarding the stable nature of business activities and the demonstration of robust controls, these criteria would be difficult to interpret and would likely be very burdensome to assess for supervisors (especially those that are responsible for supervising a high number of entities). Regarding operations in a sector identified as low risk in the national risk assessment, this criterion could hamper harmonisation at the Union level, as different Member

		States might identify different sectors as low risk.	
Article 5 Reduced frequency – Major events or developments in the management and operations of obliged entities	Some respondents claim that the notion of 'major events or developments in the management and operations of obliged entities' is not clear. Furthermore, some respondents found it unclear whether the occurrence of such events resets the assessment timeline or affects the frequency of regular risk assessments.	The notion of major events is defined in Article 4(6) of the draft RTS. The definition is deliberately broad to ensure that it can capture all events that may have a significant impact on a firm's risk profile. As indicated in Article 4(4) and (5), the occurrence of a major event shall trigger an ad hoc assessment that should be conducted in addition to the periodic assessment. The scope of this additional assessment should be limited to the impact of the major event. It is not, in principle, a full reassessment of the firm (even though supervisors may conduct a full reassessment if they deem it necessary). The objective is to ensure that supervisors can swiftly update their understanding of the risk if a significant development occurs and react accordingly where needed. Therefore, the occurrence of major event does affect the timeline of the periodic assessment.	None.

Annex 1 Lack of clarity of some data points and sector-specific needs	Several respondents said that certain data points (e.g. complex structures, high-risk activities) are not sufficiently clear, which may further complicate the data collection. In addition, some respondents said that the data points are not sufficiently adapted to the specificities of certain sectors.	The EBA agrees that the clarity and consistent interpretation of data points needs to be ensured. The EBA also agrees that it needs to be clear which data points apply to which sectors. In addition, the definitions of the data points should be adapted to the different sectors where relevant.	Addition of an interpretive note to clarify the meaning of the data points (Annex 2). Clarification of the sectors to which each data point applies in the list provided in Annex 1
Annex 1 Number of data points and burden on the industry	Several respondents expressed concerns in relation to the data points. These respondents consider that the number of data points is high. In addition, many data points are currently not available in structured formats, requiring extensive data gathering and system adaptations, which will be costly for the private sector.	Not all data points will apply to all obliged entities. The list of applicable data point will depend on the sector in which the entity operates and on the services it provides. The EBA expects that most entities will not be required to provide more than 100-150 data points, which is less than institutions currently have to provide in many Member States. Following the public consultation, the EBA removed 15% of the data points it originally proposed where consultation feedback and a data exercise involving over 100 institutions suggested that these would be insufficiently	Streamlining the list of data points and removal of the data points that are insufficiently meaningful and/or overly costly to obtain.

		meaningful or costly for the private sector in comparison to the benefits of collecting them. The remaining data points should not be difficult to retrieve for most institutions. Furthermore, and as reflected in the impact assessment available in Section 4.1, while adapting to the new framework may create costs for firms, the EBA expects that these initial costs will be outweighed by significant benefits in the long term, should the list of data points remain sufficiently stable over time. Firms' reporting obligations will be harmonised at Union level, which means that those which operate in different Member States will no longer have to report different data in those Member States. Furthermore, it will lead to a greater comparability of risk assessment outcome at Union level, which means that supervisors will be able to coordinate more easily.	
Relationship between the risk assessment methodology and the	Some respondents note that the RTS fails to clarify how supervisory assessments will relate to, and potentially leverage, existing business-wide risk assessments under Article10(4) AMLR (with AMLA guidance due by July 2026).	The risk assessment methodology under Article 40(2) AMLD6 and the entities' business-wide risk assessments aim to achieve different objectives. The former aims to inform supervisory	None.

business-wide risk assessment		decisions while the latter is a tool that entities need to use to design their AML/CFT defences.	

Responses to questions relating to the RTS on the risk assessment for the purpose of selection of credit institutions, financial institutions and groups of credit and financial institutions for direct supervision (Article 12(7) AMLAR)

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
Article 1 Materiality thresholds – Notions of 'customers' and 'transactions'	Some respondents suggested clarification for the notion of 'customers' and 'transactions'. Some respondents also suggested only considering active customers for the purposes of the calculation of the materiality thresholds.	The EBA agrees that these notions should be clarified. Regarding the suggestion to focus on active customers, the EBA is concerned that this approach would lead to unduly excluding firms which, due to the sector in which they operate or their business model, have a high number of customers that carry out transactions on an infrequent basis.	Clarification of the notions in the interpretive note (Annex 2).
Article 1 Materiality thresholds – timeframe	Some respondents underlined a lack of a clear timeframe for assessing the materiality thresholds.	The draft RTS clarify that the materiality thresholds should be assessed based on the data points in Annex 1. These data points explicitly refer to the number of customers and the value of transactions at the end of the year preceding the	None.

		assessment. It should therefore be sufficiently clear.	
Article 1 Materiality thresholds – Value of the thresholds	There is no strong consensus among respondents as to whether the thresholds should be increased or decreased. Some respondents consider that the thresholds are too low because certain activities (private banking, asset management, CASPs) would, in their view, easily exceed them. Others consider that the thresholds are too high because, in their view, only relatively large groups would exceed them. Some respondents suggested completing the quantitative thresholds with qualitative and operational risk indicators (e.g. enhanced control capabilities, actual risk profile).	Respondents did not provide evidence to support their response. In addition, the notion of 'minimum activities' used in the level 1 text entails that the assessment should be made based on quantitative factors. The values are in line with the views of national supervisors and based on their assessment of their sector. Since consultation responses were inconclusive, they will remain unchanged.	None.
Article 1 Case of branches of collective investment undertaking	A few respondents indicated that collective investment undertakings often establish branches which do not operate as distributors. These respondents suggested that these branches should not be considered as establishments under the AMLAR, nor should the collective investment undertaking be considered as operating under free provision of services through those branches.	AMLA does not have a legal mandate to specify what activities fall within the scope of the freedom of establishment or the freedom to provide services in the draft RTS. The draft RTS can only set out the minimum activities to be carried out by an institution under the freedom to provide services to be considered as operating in a Member State.	None.

Article 2 Impossibility of manually adjusting the inherent risk score	Several respondents said that there should be a possibility of manually adjusting the inherent risk score based on evidence and with certain limits, to the extent that the adjustment would be possible.	Manual adjustments of the inherent risk score could introduce discrepancies between the different Member States and hamper harmonisation.	None.
Article 5 Group-wide score – Scope of the group	Several respondents found the group perimeter unclear. They were unsure whether entities that are not credit or financial institutions should be counted. They were also unsure about the status of entities located in third countries.	The EBA agrees that the perimeter of the group should be clarified. Since AMLAR refers to credit institutions, financial institutions and groups of credit institutions and financial institutions, the EBA is of the view that only the entities that have the status of credit institution and financial institutions should be taken into account when calculating the group-wide score. As regards institutions established in third countries, no score would be available to include them in the calculation of the group-wide score under the draft RTS proposed for consultation. While the EBA sees merit in including an additional mechanism to reflect groups' exposure to third countries, such a mechanism would increase the complexity of the methodology and the burden for competent authorities and obliged entities. Furthermore, some data points	Revision of Article 5 of the draft RTS.

		(especially in the 'geographies' category) already capture risks to which institutions are exposed due to their exposure to third countries, which would create a risk of duplication. The EBA therefore proposes not changing the formula.	
Article 5 Group-wide score – Calculation of the score	Several respondents find the formula rigid, overly reliant on volume metrics (customers, transaction value, assets).	The EBA takes note of the respondents' concerns on the methodology proposed to calculate the group-wide score. In the absence of concrete suggestions as to how the formula could be adjusted and why certain adjustments would produce a better outcome, the methodology remains unchanged.	None.
Article 7 Date of application	Several respondents suggested that the envisaged timeline is overly ambitious. System adaptations and reporting workflows require significant time. One stakeholder also proposed a phased and practical approach allowing stakeholders to initially report on a best-effort basis.	The date of application of the risk assessment and selection methodology is set out in the level 1 text (Article 13 AMLAR). Therefore, it cannot be amended by a provision of the RTS.	None.

Responses to questions in Consultation Paper EBA/CP/2025/04 in relation to the RTS on Customer due diligence under Article 28(1) AMLR

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Question 1 - Identification and verification			
Article 1 Clarification on the scope of individuals to which Articles 1–5 of the RTS on CDD apply	Many respondents sought clarification on the scope of Articles 1–5 of the draft RTS and whether they apply to customers 'only', or also to '*the customer, any person purporting to act on behalf of the customer, and the natural persons on whose behalf or for the benefit of whom a transaction or activity is being conducted*', as Article 22(1) AMLR sets out.	The articles in the draft RTS on CDD that are based on Article 22(1) AMLR apply not only to the 'customer' but equally to the broader population of 'any person purporting to act on behalf of the customer, and the natural persons on whose behalf or for the benefit of whom a transaction or activity is being conducted'.	Article 1 (now Article 2) amended.
Article 1(2) Scope of non-natural persons	Respondents asked clarifications on whether the 'name of a legal entity', as referred to in draft Article 1(2) of the RTS on CDD, also applies to 'other organisations that have legal capacity under national law', as referred to in Article 22(1)(d) AMLR.	The EBA confirms this understanding.	Article (1)(2) (now Article 2(2)) amended.
Article 1(2) Clarification on the legal entity's 'commercial name', in addition to its 'registered name'	Several respondents considered that the draft RTS go beyond the AMLR requirements by requesting that the 'commercial name' of the legal entity is obtained, when the commercial name is different from the 'registered name' of the legal entity. They indicated that this information is difficult to obtain as it is not always mentioned in the official documents.	Article 1(2) of the draft RTS on CDD serves to clarify how to comply with the requirement to obtain the 'name of the legal entity' as referred to under Article 22(1)(b)(i). The use of 'commercial name', also called 'trade name', is not consistent across EU Member States (MS) for commercial or marketing reasons. In certain MSs, more than one 'commercial name' can be allocated to one 'registered name'. Collection of the 'commercial name', when it differs from the registered name, also has an additional value for Targeted financial sanctions (TFS) screening purposes. The benefit of obtaining the information on the "commercial name" is accordingly deemed higher	Article (1)(2) (now Article 2(2)) amended.

		than the costs of obtaining it – the 'commercial name", when it differs from the "registered name", can be collected from the customer in the form of a written declaration. The term "commercial name" has been changed to 'trade name" to align with other EBA regulatory products.	
Article 3 Interpretation of the place of birth	Many respondents indicated a high cost for obtaining the information on the city of birth of the customer. They indicated that not all ID documents contain both the country and the city of birth, which would then: 1. Increase the risk of financial exclusion, 2. Put additional burden on obliged entities (OEs) to ask for a second ID document for the purposes of obtaining information on the city of birth. Respondents also claimed that the value added of knowing the customer's city of birth is minimal for AML/CFT purposes..	The AMLR requests, under Article 22(1)(a)(ii), that institutions obtain the 'place and full date of birth'. Based on the costs associated with collecting the 'city of birth' and the benefits of obtaining such information from an AML/CFT perspective, the EBA clarifies that *at least* the country of birth should be collected by the OE to determine the 'place of birth'.	Article 3 (now Article 4) amended.
Article 4 Obtain information on the nationality, or nationalities of customers	Several respondents indicated that obtaining information on the nationality, or nationalities, of the customers is complicated. They indicated that some identity documents (e.g. driving licences) may not contain information on nationality. Some respondents questioned the value added of obtaining information on nationality for the purpose of ML/TF risk mitigation. Others mentioned that requiring the nationality of the client may seem discriminatory.	OEs must obtain the nationalities of their clients according to Article 22(1)(a)(iii) AMLR. Being a specific provision in an EU regulation, the draft RTS cannot ease this requirement. Nationalities (or, alternatively, statelessness and refugee or subsidiary protection status, where applicable) must be obtained in line with AMLR. However, there is no obligation for OEs to collect specific documentation for each nationality of the customer (i.e. no requirement to obtain one passport for each); a declaration from the customer would be sufficient for multiple nationalities.	Article 4 (now Article 5) amended and Recital 3 added.
Article 5(1) Features a document should contain to be considered as	Respondents indicated that the list of conditions under Article 5(1)(a)-(g) do not feature in all ID documents issued and used in EU Member States. Defining	Article 5(1)(a)-(g) establishes an exhaustive list of features that a document must contain in order to be treated as equivalent to a passport or a national identity document for the purposes of verifying a natural person's identity, in line with Article 22(1)(a) AMLR. The list	Article 5(1) (now Article 6(1)) amended.

equivalent to an ID document or passport	an 'equivalent' document on this basis would put the bar higher for 'equivalent' documents than what is included in actual national ID documents or passports. According to the respondents, since many natural persons who lack ID documents also do not have documents that meet the requirements to be 'equivalent' documents, this provision is too prescriptive, on the one hand, and on the other hand could also lead to financial exclusion. In particular, criticism from respondents concentrated on points: (b) on 'place of birth' and on 'nationality', (e) machine-readable zone and (g) on biometric data.	has been revised, in light of the responses received through the public consultation. Changes included the deletion of the reference to the 'nationality' and the 'place of birth' from the list of features, taking into account that not all government-issued identity documents contain information on the holder's nationality or their place of birth.	
Article 5(2) to further enhance the principle of financial inclusion	Respondents indicated that the list of requirements is too long and burdensome to be obtained under Article 5(2) of the RTS for natural persons who have legitimate reasons for not being able to provide either an ID document, passport, nor an 'equivalent' document (for example, asylum seekers, refugees, persons to whom a residence permit has not been granted, but whose expulsion is impossible for legal or factual reasons; homeless people or otherwise vulnerable persons). Respondents indicated that, in order to enhance financial inclusion, there should be simplified measures for the purposes of identification and verification for this specific group of natural persons.	AMLR does not provide an exemption from the information, as listed under its Article 22(1)a, to be collected by OEs for vulnerable groups of natural persons, such as asylum seekers, refugees, persons to whom a residence permit has not been granted, but whose expulsion is impossible for legal or factual reasons; homeless people or otherwise vulnerable persons. To mitigate the risk of financial exclusion and unwarranted de-risking, while still being compliant with AMLR, these RTS allow OEs to obtain the requested information from these natural persons via other credible means, including via declaration.	Article 5(2) (now Article 6(2)) amended and Recital 7 amended.

Article 5(5) 'Original' or 'certified copy' of the ID documents, passport or equivalent	Respondents indicate that requesting the 'original' or the 'certified copy' of the ID documents, passport or equivalent is disproportionate and an unnecessary administrative burden, which may also not be operationally feasible in certain sectors outside the banking sectors (e.g. the asset management industry). They also claimed that it goes beyond the wording of Art 22(6)(a) AMLR.	Measures for verification of the ID document, passport or equivalent are split between Article 6 (face-to-face situations) and Article 7 (non-face-to-face situations) of the draft RTS. In a face-to-face situation, the natural person will need to present either the original copy of their ID document, passport or equivalent, or, if these are unavailable for a plausible reason, a certified copy of the ID document, passport or equivalent. In the case of non-face-to-face situations, the verification measures are set out under Article 7 of the draft RTS instead.	No amendments made.
Article 5(4) 'Certified translation'	An overwhelming number of respondents questioned the insertion of the mention of 'certified translation" under Article 5(4) of the draft RTS when referring to methods OEs should use to understand the content of original documents which are in a foreign language. Respondents criticised that several other means of translation can provide the same results, for example digital translation tools or other existing internal practices (e.g. translation through employees speaking the language in question).	The EBA decided not to specify, within the RTS, any methods for satisfying the requirement of understanding the content of original documents which are in a foreign language. Instead, the responsibility on *how* to understand such content remains with the OEs, provided that OEs, at any moment, are able to demonstrate to their competent authority that the method they use for translating documents in foreign language is reliable and robust. The reference to 'certified translation' has been deleted from Article 5(4) of the RTS.	Article 5(4) (now 6(4) amended).
Article 9 Clarification of measures under Article 9 a) and b) should be read cumulatively	More than one respondent indicted that it would be helpful to clarify that this list of the 'reasonable measures" under Article 9, is a) to be applied on a risk-sensitive manner, and b) that the list is non-exhaustive, and that the different registers mentioned under Article 9(a) are not to be consulted cumulatively.	The EBA confirms that the measures under Article 9(a) and (b) are risk-sensitive, non-exhaustive, and that the consultation of the different registers is not cumulative. The language has been adjusted by adding 'one of the following measures', and by replacing 'and' by 'or' throughout.	Article 9 (now Article 10) amended.
Article 9(b)	Two respondents suggested including reputable credit agencies and/or	EBA accepted the proposal and added reputable credit agencies and/or comparable data services providers to Article 9(b).	Article 9(b) (now Article 10(b)) amended.

Credit agencies as additional source of information	comparable data services providers as another example of reliable source of information under Article 9(b) of the RTS.		
Verification of the UBO in low-risk situations, Article 9 of draft RTS	In relation to Article 9, some respondents suggested that, in their view, in low-risk situations, verification of the identity of the beneficial owner should not be necessary at all (for example for inoperative entities, public entities, listed companies, etc.) and that Article 9 should clarify this.	Article 9 of the draft RTS specifies what are the reasonable measures for verification of the UBO in accordance with the requirements of Article 22(7)(b) AMLR. For verification of the UBO in low-risk situations, the RTS have a dedicated Article 19 under Section 4.	No amendments made.
Article 10(1) Risk sensitiveness of the measures for understanding the ownership and control structure of a customer that is not a natural person	Respondents indicated that the language of Article 20(1)(b) AMLR, explicitly referring to 'taking reasonable measures', follow the risk-based approach; however, the language of Article 10 of the RTS does not. Therefore, they considered that the list of information under Article 10(1) would be disproportionate for standard or low-risk situations. Such granular information on all intermediate entities, as some respondents indicated, is also not requested for the national UBO registries. Moreover, they indicated that compliance with the requirement to understand the ownership and control structure does not necessarily require an assessment of the entire structure of the legal entity customer by the obliged entity. There were several respondents who indicated that the wording of 'intermediary connections" is also unclear, as it is not an AMLR term.	The language of Article 10(1) has been adjusted to limit the scope of the information to intermediate entities that are relevant for the understanding of the ownership and control structure. The terminology of 'intermediary connections" has been replaced with "intermediate entities", which is an AMLR term.	Article 10(1) (now Article 11(1)) amended.

Article 10(1)(c) Information requested on the regulated market under this Article	Several respondents indicated that information requested under Article 10(1)(c) is publicly available information and therefore they deemed it would be unnecessary to request from the customer.	The language of the *chapeau* under Article 10(1) of the RTS indicates that OEs shall [take risk-sensitive measures to] 'obtain' the information listed. It is not required that all this information shall be requested from the customer if it can be obtained by other means.	No amendments made.
Article 11(1) Notion of 'complex structures'	Several respondents challenged the definition introduced by the RTS of 'complex structures'. In relation to the 'two or more lawyers' between the customer and the UBO, they indicated that the economic reality of legal entities is that they usually have two or more such lawyers. In addition, respondents believed that points a) to d) should not be looked at individually but in a cumulative manner if 'one or more' of these elements are met. They indicated that the current definition, if maintained, would capture too many legal entities as 'complex structures", which is not the intention of this Article. Some clarifications were also requested on the meaning of 'different jurisdictions' under Article 11(1)(b) – i.e. as to whether this refers to jurisdictions outside the EU or rather to high or higher risk jurisdictions.	The features, as described under a) to d) of Article 11(1) of the draft RTS have been revised in a way that does not capture a disproportionally high number of legal entities as 'complex structures'. In addition, the EBA clarified that 'different jurisdictions' under Article 11(1)(b) refers to jurisdictions outside the EU. The EBA also clarified that legal entities which are identified by the definition under Article 11 as 'complex structures' do not automatically trigger enhanced due diligence measures. To better differentiate the wording, and thus avoid any possible confusion with 'excessively complex ownership structures', which are mentioned under Annex III AMLR as higher risk factors, the terminology has been changed from 'complex structures' to 'complex corporate structures' in the RTS.	Article 11(1) (now Article 12(1)) amended.
Article 11(2) Requirement to obtain an organigram for complex structures	Some respondents questioned why the additional information to be obtained from a legal entity which is a 'complex structure' would be an 'organigram', and why the draft RTS would leave it as more flexible for the obliged entity to decide what 'additional' information it will need	The language of Article 11(2) of the draft RTS has been revised to provide for a more flexible approach to what additional information the obliged entity can request in case of complex corporate structures.	Article 11(2) and (3) (now Articles 12(2) and (3)) amended.

	to obtain. Some respondents mentioned that it can be redundant and hence disproportionate to always request an organigram.		
Article 12 Information to be collected on Senior Managing Officials (SMOs)	Several respondents questioned the fact that the same information as for UBOs as requested under Article 62(1)(a) AMLR should be required as information to also be collected for the SMOs. They argued that if that had been the explicit policy choice, then Article 22(2) AMLR would clearly state it. They explained that this approach raises questions about the purpose of collecting such information, and would also raise other issues related to data privacy. For example, requesting the residential address of SMOs would be disproportionate and add no value for mitigating ML/TF risks.	Recital 125 AMLR confirms that SMOs are not UBOs. Article 63(4)(b) AMLR indicates that, for SMOs, information to be collected should be 'equivalent information' to Article 62(1) AMLR. In line with this, the EBA clarified in the final RTS that the address of the registered office can be collected instead of the SMO's residential address and country of residence. In addition, Recital 11 has been included to clarify these aspects.	Article 12(a) (now Article 13(a)) amended, and Recital 11 added.
Article 14 Discretionary trusts	At least four respondents indicated that measures under Article 22(5) AMLR are risk-based, and the EBA should acknowledge this explicitly in the language of Article 14.	The EBA agrees and adjusted the text of Article 14 of the draft RTS accordingly.	Amendments made to Article 14 (now Article 15).
Exemptions from AMLR requirements for specific types of institutions and firms	Some respondents were asking for certain exemptions from certain AMLR CDD requirements for certain types of OEs. Examples: crowdfunding platforms or NPOs, arguing that it would imply high compliance costs.	OEs under the AMLR are listed in Article 3 AMLR. Unless otherwise specified in specific AMLR articles, provisions of the AMLR will apply to this list of OEs. The RTS, as a Level 2 instrument, cannot create exemptions from the application of the Level 1 text (i.e. the AMLR).	No amendments made.

Question 2 - eIDAS

Article 6(2) Non-eIDAS solutions to be recognised, by the RTS, as equal alternative to eIDAS solutions.	The majority of respondents requested that non-eIDAS solutions should be recognised as an equal alternative to eIDAS solutions, instead of only accepting them if the eIDAS solution is not available or cannot be reasonably expected to be provided. If this approach is not possible, then these respondents requested a transitional period.	The EBA RTS reflect the EU COM's reading of the AMLR, according to which eIDAS solutions should be used by OEs.	No amendments made.
Article 6 Applicability to natural persons only	Some respondents suggested limiting the scope of the entire Article 6 of the draft RTS in a way that it should apply only to natural persons and not to customers which are legal entities.	The EBA's RTS are built on the EU COM's interpretation in this regard – which indicated that the eIDAS-compliant solutions apply to natural persons but also to legal entities (with some time lapse in the application and priority given to individuals).	No amendments made.
Article 6 Application to customers *only* or to all the population captured by Article 22(6) AMLR	Respondents enquired as to whether Article 6 applies to 'customers' only or equally to 'any natural person purporting on their behalf', as indicated in Article 22(6) AMLR.	The EBA confirmed that Article 6 applies to customers, but also to 'any person purporting to act on their behalf', as indicated under Article 22(6) AMLR.	Article 6(2) (now Article 7(2) amended.
Article 6(3) Enquiries around the "consent" of the customer and its necessity	Respondents raised a lot of uncertainties on why specific consent is requested under this specific article and not specifically mentioned for others. Respondents claim it is duplicating efforts and thus increasing costs. In addition, asking for consent would also imply that the customer may be able to subsequently revoke this explicit consent, which would then be contradictory, according to certain respondents, with Article 76 AMLR. Lastly, some also indicated that such explicit consent is not requested for the	The specific reference to requesting consent, and recording such consent, has been deleted from Article 6.	Article 6(3) deleted.

	eIDAS tools, so it is not clear why it should specifically be asked for the non-eIDAS tools		
Article 6(4)(b) Reference to "audiovisual communications" and "end-to-end encrypted video chats"	Non-banking sector respondents pointed out that the language referring to "audiovisual" communications is overly prescriptive, not technologically neutral and favours live data streams. As such, they highly limit the choice of technological solutions that could be used, which would be unjustified for certain sectors. In addition, as they indicated, these requirements would not be suitable for the identification of legal entities and natural persons acting on behalf of them.	The EBA agrees to use a more natural language under Article 6(4)(b); the references to "audiovisual" as well as to the "end-to-end encrypted video chats" have been deleted.	Article 6(4)(b) (now Article 7(3) amended.
Article 6(5) Verification of security features, as presented by a non-natural person customer	Respondents claim that the specific requirement to verify security features is not feasible in a non-face-to-face context (i.e. reproductions (. copies) of original documents may not contain security features such as holograms).	OEs should refer to paragraph 33 of the EBA Guidelines on remote onboarding to get more guidance on how the reliability of reproductions can be assessed. The reference to 'verify' has been replaced by 'take reasonable steps to ascertain'.	Article 6(5) (now Article 7(4)) amended.
Question 3 - Virtual IBANs			
Article 8 Request for more clarification on the terms, roles and responsibilities as well as more details and guidance requested in specific regulations	Several respondents requested that the EBA to provide more clarification on the terms, roles and responsibilities referenced in Article 22(3) AMLR and the draft RTS. Respondents also felt that the use of virtual IBANs should be more detailed in regulations for credit institutions or financial institutions, to effectively mitigate the risks associated with virtual IBANs, with some respondents requesting	The EBA agrees that more clarification would be helpful in relation to virtual IBANs to allow for the legitimate benefits of virtual IBANs and the effective mitigation of any AML/CFT risks. However, considering the legal constraints of the mandate to only specify the information to be collected pursuant to Article 22 AMLR as well as the technicality of virtual IBANs and the various use cases, further clarification should be considered by the co-legislator.	No amendments made.

	stronger attribution, transparency and risk monitoring standards.		
Article 8 Information to be collected for identifying and verifying the identity of the natural or legal persons using the virtual IBAN	Respondents requested clarification on what information is required for identifying and verifying the identity of the natural or legal persons using the virtual IBAN as mentioned in Article 22(3) AMLR.	The EBA provided clarity by specifying the information to be obtained to identify and verify the identity of the natural or legal persons using the virtual IBAN, which is the same information as mentioned in Article 22(1) AMLR.	Article 8 (now Article 9) amended.
Article 8 Clarification on whether the EBA intended to codify a three-party model for the issuance and usage of virtual IBANs or to enable a more complex four-party model	Respondents asked the EBA whether it intended to codify a three-party model for the issuance and usage of virtual IBANs or to enable a more complex four-party model that introduces an additional layer between financial institutions and the end-users. Other respondents mentioned that such a four-party model was either not allowed in their jurisdictions or was something they would not want.	The EBA clarifies that, in line with its mandate given by the co-legislator, the principle of simplification, and considering the uncertainty in relation to certain terms used in Article 22(3) AMLR, the EBA amended the proposed Article 9 of the draft RTS to ensure it is in line with the mandate of Article 28(1) AMLR.	Article 8 (now Article 9) amended.
Article 8 Application of the scope of the RTS as this includes both natural *and* legal persons using a virtual IBAN.	Some respondents flagged the difference in scope between the AMLR and the RTS. The RTS includes both the 'natural person' using that virtual IBAN as well as the 'legal persons' using the virtual IBAN, whereas Article 22(3) paragraph 2 AMLR does not include legal persons.	The EC will issue a corrigendum to include the term 'legal persons' in Article 22(3), second paragraph, AMLR. In anticipation of this corrigendum, the EBA has already catered for this by also including legal persons in the RTS.	No amendments made.
Question 4 - Purpose and intended nature of a business relationship or occasional transaction			
General comment Risk-based application	Several respondents commented that, in their view, the proposed Articles 15 and 16 of the draft RTS are highly prescriptive and not in line with the risk-based	The EBA clarifies that the RTS should always be read together with the applicable Level 1 text. Articles 20(1)(c) and 25 AMLR allow for a risk-based application. This means that OEs are required to obtain the information – in line with Level 1 – only w*here necessary*.	Articles 15 and 16 (now Article 18) and current Recital 12 amended.

	approach. For example, they argued that the wording of the draft RTS implies that all information listed should always be collected, in spite of the Regulation (EU) 2024/1624 requiring OEs to obtain information on the purpose and intended nature of a business relationship or occasional transaction 'where appropriate'. Some respondents also mentioned that their products or services are self-explanatory or that the purpose and nature is evident from the product/service itself, which, in their view, does not require further information to be collected as required by the draft RTS, or they requested to only obtain some of the information as set out in the draft RTS, tailored to the specific situation. Finally, respondents also flagged the overlap between Article 15 and 16 of the draft RTS, suggesting merging these articles to ensure further clarity.	For example, when an obliged entity assesses that it lacks an understanding of the business activity of the customer, it needs to obtain some or all of the information mentioned in the current Article 18 of the draft RTS as proportionate to mitigate the risk posed by the customer before entering into a business relationship or performing an occasional transaction. By contrast, inferring the purpose and intended nature from the type of transactions or business relationship established is limited to situations to which Article 33 AMLR applies. The EBA amended Recital 12 accordingly. To ensure maximum clarity, the former Articles 15 and 16 are amended and restructured to make the risk-based approach more explicit. Additionality, the EBA agrees that the current Articles 15 and 16 of the draft RTS could benefit from more clarity if these two Articles were merged into a single Article. Finally, the EBA included a new Article 1 underlining proportionality and the risk-based approach.	
General comment Clarification of terms and applicability	Some respondents requested further clarification of some of the terms used in the former Articles 15 and 16 of the draft RTS to ensure that the information collected is relevant and useful. Respondents also requested clarification on whether some of the defined information to be collected in the RTS should be collected by all OEs, or some, or whether the requirements apply	The EBA agrees that the wording of the former Articles 15 and 16 could be further enhanced by using more precise language to improve understanding, convey intent and ensure that the information collected is relevant and useful. That is why the EBA streamlined, merged, amended and restructured these articles, and aligned them with Level 1 terminology to the greatest extent possible. The EBA clarifies that the information to be collected is relevant for all OEs, as defined in Article 3 AMLR, taking into account their specific business models. While the focus was primarily on the financial sector, the RTS – in line with Article 25 AMLR – do not exclude any	Articles 15 and 16 (now Article 18) amended.

	systematically, or only in certain circumstances.	category of OEs, nor do they distinguish between legal and natural persons. Where possible, the EBA clarified which information is to be collected for legal persons and which for natural persons.	
Article 15(c) Information on whether the customer has additional business relationships with the obliged entity or its wider group	Respondents commented that this requirement would be challenging to comply with, citing practical and proportionality concerns as well as GDPR-related challenges. Consequently, respondents asked the EBA to limit the requirement to business relationships with the obliged entity or OEs subject to AML requirements, to delete the requirement or suggested including wording such as 'where applicable', 'where relevant', and/or 'on a risk-based approach'.	The EBA clarifies that Article 16(3) AMLR states that the policies, procedures and controls pertaining to the sharing of information referred to in paragraph 1 of that Article shall require OEs within the group to exchange information when such sharing is relevant for the purposes of customer due diligence and money laundering and terrorist financing risk management. Against this background, the EBA sees merit in OEs, especially at the onboarding stage, requesting, where relevant, whether the customer has additional business relationships with the obliged entity or its wider group. This can provide valuable information on the risk posed by the customer, which will allow for tailored mitigating measures and possibly reduce duplication of efforts and costs where customer due diligence checks are already performed elsewhere in the group or obliged entity. Finally, the EBA amended the article in line with suggestions from respondents to cater for situations in which the obliged entity is not part of a wider group.	Article 15(c) (now Article 18(a)(iv)) amended.
Article 15(d) Proportionate application of source of wealth	Several respondents, referencing the AMLR, remarked that determining the source of wealth might be better suited in the section on enhanced due diligence measures instead of in the section on purpose and intended nature, with some citing that it should not be a standard requirement but instead applied selectively. Therefore, they asked for it to be deleted.	To ensure a clear application of this requirement, the EBA removed this requirement from the purpose and intended nature section of the RTS. Nonetheless, even in cases of standard due diligence, determining the source of wealth may be necessary to understand the customer's ML/TF risk profile. The co-legislators recognise this by requiring, as an enhanced due diligence measure, OEs to obtain, in proportion to the higher risks identified, *additional* information (i.e. where necessary it should have been determined already) 'on the source of funds and source of wealth of the customer and of the beneficial owners'. Therefore, an enquiry into the source of wealth of the customer and of the beneficial owners can be an appropriate and proportionate measure to identify and mitigate ML/TF risks, even in CDD situations.	Article 15(d) (now Article 18) amended.
Article 16(d)	Some respondents found identifying expected recipients, jurisdictions and intermediaries impractical, explaining	Article 25(d) AMLR is clear that, before entering into a business relationship or performing an occasional transaction, an obliged entity shall assure itself that it understands its purpose and intended	Article 16(d) (now Article 18(d)(iii)) amended.

Clarification in relation to the destination of funds	that customers will not be able to provide this level of specificity, claiming rising compliance costs, at least for retail customers, and also asking for examples of indicative categories.	nature. To that end, an obliged entity shall obtain, where necessary, information on the destination of funds, for which the RTS – in line with Article 28(1)(a) AMLR – defines the information to be collected. This information should be aligned with the customer's risk level. Collecting this information should also be feasible for retail customers, e.g. by identifying types of recipients in case of payments or value transfers. In addition, and to further clarify its intent, the EBA amended this requirement by including as a source of information whether the recipient of funds is the intended beneficiary of the transferred funds or is acting as intermediary for the beneficiary.	
Article 16(e) Clarification in relation to the business activity or the occupation of the customer	Some respondents requested to delete *'key stakeholders'* or insert 'where available' as they see this information as not critical where sufficient information on the industry and products/services has been obtained or deemed excessive. Respondents also requested further clarification on whether the information to be collected under the former Article 16 point (e) of the draft RTS only refers to the customer's employment status (e.g. employed, unemployed, etc.), or whether this also includes any further information.	The EBA clarifies that *key stakeholders* are individuals or entities that, because of their close relationship with the customer, may impact the risk profile of the customer. The collection of this information allows for a risk-based application, which is made more explicit by the restructuring of the current Article 18. In relation to the occupation of the customer, the employment status alone may be sufficient in some situations. By contrast, in other situations the sector of employment, or previous sector in case of retirement, can provide relevant information for AML/CFT purposes. The RTS leave sufficient flexibility for OEs to tailor their measures to the specificities of the situation.	Article 16(e) (now Article 18(e)) amended.
Question 5 – Politically Exposed Persons (PEPs)			
Article 17 Screening of senior managers officials (SMOs)	Many respondents asked for clarification on whether the senior managing officials (SMOs) must be subject to PEP screening, according to the new European legal framework.	Article 20(1)(g) AMLR requires PEP screening for the customer, their beneficial owners, and, where relevant, the person on whose behalf or for the benefit of whom a transaction or activity is conducted, but it does not explicitly include senior managing officials (SMOs). In contrast, Article 22(2) AMLR requires identifying and also verifying SMOs. Furthermore, given that Recital 125 AMLR clarifies that SMOs are not beneficial owners, it can be concluded that PEP screening for	No amendments made.

		SMOs can be performed on a risk-sensitive basis, but it remains highly relevant for assessing the customer's overall risk profile.	
Article 17(1) Reference to the AMLR definition of PEP	Respondents asked to confirm that, for the application of the RTS, the definitions of *family member* and *close associate* of a PEP should be limited to those in Article 2 (1), points 35 and 36, AMLR.	As a general rule, the provisions of the RTS should be read in conjunction with the AMLR. The preamble of this article has nevertheless been amended, adding references to ensure consistency with the AMLR and to clarify that the screening under Article 17 of the RTS refers exclusively to the categories defined in Article 2(1), points 35 and 36, AMLR.	Article 17(1) (now Article 19(1)) amended.
Article 17(1)(a) Time of screening	Respondents requested clarification on whether the screening of customers must be completed prior to establishing a business relationship, or whether an initial self-declaration is sufficient, with subsequent monitoring carried out via batch-based automated screenings.	As a general rule, under Articles 19 and 20 AMLR, PEP screening must take place before a business relationship is established or before carrying out an occasional transaction. Determining whether a customer is a PEP is central to assessing overall risk and forms a key part of ongoing monitoring. Where a person is identified as a PEP, enhanced due diligence – including senior management approval – is required before onboarding. Consequently, postponing screening until after onboarding would mean entering into a relationship without the necessary safeguards.	No amendments made.
Article 17(1)(b) Triggers upon which the PEP screening must be conducted	Respondents suggested that the triggers in paragraph 1(b) are too narrow, relying mainly on infrequently updated EU lists, and suggested that the RTS explicitly include political events – such as elections, cabinet reshuffles, or constitutional changes – as additional triggers for PEP re-screening, even if Member State lists have not been updated. In addition, they requested clarification on what should be intended as a significant change that should trigger a new PEP screening.	The RTS are intentionally formulated in broad terms, with categories designed to also capture situations beyond those explicitly listed. This approach ensures that, for example, according to a risk-based approach, following political events such as elections or cabinet reshuffles, OEs assess whether an individual has become a PEP, even where national lists have not yet been updated. With regard to re-screening, it should occur when the changes could affect a person's PEP status (e.g. elections, changes in ownership or public functions), but not for minor updates (e.g. address or contact details). The EBA has amended the provision to clarify that only changes with a potential impact on PEP qualification trigger new screening.	Article 17(1)(b) (now Article 19(1)(b)) amended.
Article 17(2) Manual screening	Some respondents suggested a stronger recognition of the use of automated screening processes and pointed out that	Automated PEP screening systems are the preferred approach, enabling timely and comprehensive checks, though they may not always be proportionate. This may be the case for small or less complex businesses. This aligns with FATF Recommendation 12,	No amendments made.

	manual checks should never be treated as a viable standard approach.	which expects risk management systems to identify PEPs, with purely manual checks acceptable only if demonstrably proportionate, effective and appropriate to the risk level.	
Questions 6 and 7 – Simplified due diligence measures			
Article 18(1)(a) Minimum information to be collected	Some respondents considered SDD information requirements too broad and not fully aligned with proportionality, suggesting that place of birth and nationality should not be collected.	As explained above in this table in relation to Question 1 of the public consultation, OEs must obtain information for natural persons in compliance with Article 22(1)(a) AMLR. The draft RTS on CDD cannot ease that requirement.	No amendments made.
Article 18(1)(a) Information to be collected on natural persons	Some respondents sought confirmation that national ID numbers and residence details are not required in low-risk cases, while some questioned the omission of 'usual place of residence', given its relevance for risk assessment and profiling.	The EBA clarifies that this provision sets out the information considered necessary for identification in low-risk scenarios. National ID numbers and place of residence have been carved out from Article 22(1)(a) AMLR and are not therefore mandatory in those cases, but OEs may collect additional information if necessary for a more comprehensive risk assessment and customer profiling.	No amendments made.
Article 18(1)(b) Information for the identification of legal entities	Some respondents observed that collecting the registration number, the tax identification number and the LEI are not commensurate to low risk.	The EBA has amended the provision for greater clarity, specifying that in these cases it is sufficient to obtain just one of the following: the registration number, the tax identification number, or the LEI, where applicable.	Article 18(1)(b) (now 20(1)(b)(iv)) amended.
Article 19 Identification of the beneficial owners in low-risk situations	Many respondents asked for confirmation that, in the case of low-risk customers, the consultation of the central register (or a statement from the customer) is sufficient to determine the beneficial owner, without the need for additional verification measures, provided there are no concrete indications of discrepancies.	According to Article 22(7)(b) and Recital 54 AMLR, beneficial owner registers may serve as a source to identify or cross-check information but should not be the primary source for verification. The EBA has restructured the provision to clarify that, in low-risk cases, beneficial owner identification may rely on sources under points (a), (b) and (c), while verification may use sources under (b) or (c). To facilitate the process, point (b) has been reformulated in broader terms to ensure that OEs may also rely on information they already hold.	Article 19 (now Article 21) amended.
Article 20 Sectoral SDD measures for pooled accounts	Many respondents requested an explicit exclusion from the application of this provision for payment institutions (PIs) and electronic money institutions (EMIs),	According to Article 20(1)(h) and 28(1)(b) AMLR, this provision is intended to target situations where CDD obligations are needed to identify and assess the risk of the persons on whose behalf or for the benefit of whom a transaction or activity is carried out.	Recital 15 (now Recital 17) amended.

	since in these cases the payment service is not undertaken for the benefit of a final customer, but rather for the benefit of the PSP and the implementation of this rule might cause de-risking of PIs and EMIs.	The EBA acknowledges that the relationships between a credit institution (which opens a pooled account) and a PI or EMI should be more appropriately assimilated to correspondent relationships within the meaning of Article 2(22) point (b) AMLR. As such, they fall outside the scope of this specific provision of the RTS. Given that payment services are not provided for the benefit of final customers, but for the benefit of the payment service provider itself, the rationale under Article 20(1)(h) AMLR for applying this provision would not be engaged. A clarification to this effect has been added to Recital 17.	
Article 20 Extension of the sectoral SDD measures for pooled accounts	Many respondents requested the possibility of applying the simplifications provided by this Article to other forms of pooled accounts, which generally present low risk but are opened by credit institutions to customers who are not OEs (e.g. collective rent deposit accounts, escrow accounts, accounts for school classes, etc.).	The application of the sectoral simplified due diligence measures, as defined by the RTS on CDD, is possible to the extent that the accounts in question are opened by a credit institution (as an obliged entity) with another obliged entity, which is particularly reliable as it is: 1) subject to the same AML/CFT regulatory framework as the credit institution (or, in any case, to equally robust rules); and 2) supervised, thereby ensuring compliance with these rules. A non-obliged entity could not guarantee that CDD on final customers is performed adequately; therefore, the credit institution could not rely on such an entity.	No amendments made.
Article 21 Sectoral SDD measures for collective investment undertakings (CIUs)	Many respondents requested that, provided all other conditions of the article are met, CIUs should not be required to perform CDD on all final investors, not only in low-risk cases, but also in standard risk situations, obtaining in both cases relevant information from the distributing credit or financial institutions without undue delay and upon request.	The EBA acknowledges the need for proportionality and consistency in applying CDD obligations for CIUs, given the structural characteristics of this market, where CIUs perform CDD on credit or financial institutions and rely on these OEs, as they cannot systematically identify final investors. In line with the principle of proportionality, the EBA acknowledges the possibility of applying lighter provisions not only in cases of low risk, but also in standard risk scenarios. From a legal perspective, Article 22(7) AMLR does not prescribe specific methods for verifying the identity of the persons on whose behalf or for the benefit of whom a transaction or activity is conducted, but only requires that OEs take reasonable measures to obtain the necessary information from the customer or other reliable sources. Under Article 76 AMLR, OEs may process personal data only for AML/CFT purposes, and any processing for incompatible or commercial purposes is prohibited.	Article 21 (now Article 17) amended.

		The risk-based approach must always be applied and, therefore, where there is a suspicion of high ML/TF risk, the simplification will not be applicable. Since the article now also covers standard scenarios, it has been moved from the Section on SDD to the Section on identification and verification, as a standalone article for CIUs.	
Article 21 Sectoral SDD measures for collective investment undertakings (CIUs)	Some respondents requested that the credit or financial institution distributing the CIU's units should be subject to AML obligations that are 'comparable', rather than 'not less robust', to those required by the AMLR.	The term 'no less robust' is preferable to 'comparable'. While comparable' may appear clearer, 'no less robust' – in line with the terminology used in the AMLR – ensures legal certainty by setting a clear minimum standard and avoiding weaker interpretations of third country AML/CFT requirements. By contrast, the term 'comparable' could be interpreted more flexibly, potentially weakening the standards.	No amendments made.
Article 22(2) Obligation to keep the documentation up to date	Some respondents proposed to remove the wording 'at all times' in relation to the obligation to keep the documentation up to date, since this could be interpreted as requiring OEs to permanently check that the customer information is up to date, which would be very onerous and costly and not risk-based.	The obligation to keep the documents, data or information, and the timeframe for updating customer identification data, are set out in Article 26(2) AMLR. A specific reference to this article has been inserted into the paragraph, which has also been amended to avoid redundancy and overlap with Article 33 of the RTS on CDD in relation to the transition period.	Paragraph 2 (now of Article 23) amended.
Article 23 Inferring the purpose and intended nature from the type of transactions or business relationship	Some respondents requested clarifying that the assessment of the purpose and intended nature in low-risk situations may, in certain cases (e.g. life insurance products), be derived directly from the characteristics of the chosen product or service or based on assumptions about how customers normally use the products.	The EBA clarifies that the provisions of the RTS must be read in conjunction with the rules of the AMLR. Article 33(1)(c), which is expressly referred to in the text, already provides, in low-risk situations, for the possibility of inferring the purpose and intended nature of the business relationship or occasional transaction from the type of transactions or business relationship established.	No amendments made.
Article 23 Information on the source of funds	Some respondents stated that, in low-risk situations, the source of funds information should not be required.	The EBA supports a proportionate approach whereby, in low-risk situations, OEs should collect source of funds information only where necessary to understand the relationship or resolve specific concerns. The provision has therefore been amended to avoid	Article 23 (now Article 24) amended.

		unnecessary burden while preserving flexibility to obtain source of funds details when justified.	
Question 8 - Enhanced due diligence measures			
General comment EDD obligations should be only illustrative and allow for a risk-based approach	Although respondents understand the need for broader harmonisation within the EU, some commented that the enhanced due diligence (EDD) obligations should be only illustrative, not mandatory and allow for a risk-based approach. In their view it should be left to the responsible OEs' risk-based approach, commensurate to their risk appetite, to define the precise and tailored measures to apply to each case. They propose to replace the terms 'shall', and 'at least' with 'should', or 'where necessary'. This would ensure that the requirements in the EDD section of the RTS are not misunderstood as a mandatory application of all measures defined, as this could result in undue burden.	The EBA clarifies that Article 34(4) AMLR states that in cases of higher risk, as referred to in paragraph 1 of that Article, OEs *shall* apply enhanced due diligence measures, proportionate to the higher risks identified, which *may* include the measures mentioned in points (a) to (g) of Article 34(4) AMLR. This means that in cases of higher risk EDD is obligatory, but the exact measures are for OEs to decide. However, when an obliged entity decides to apply any of those measures specified in Article 34(4)(a) – 34(4)(g) AMLR, the RTS specify the information that OEs shall at least collect for these measures. Therefore, the current Articles 25–28 of the RTS leave room for a targeted, tailored and risk-based approach. The EDD section of the RTS does not require that *all* additional information specified is collected in each and every case, as there may be situation where the existing information already held by OEs may already go some way to meeting the specific requirements and mitigate the higher risk identified, nor dos the RTS intend to make all measures of Article 34(4) AMLR mandatory. The EBA has amended Articles 25–28 of the RTS to make this more explicit.	Current Articles 25-28 amended.
General comment Requested exemption for Non-Profit Organisations (NPOs)	Some NPOs requested exemption from some of the EDD Articles in the RTS. For example, an exemption from the requirement in Article 26, point (a), of the draft RTS to provide proof of income for non-profit-related accounts, stateless and forcibly displaced individuals. Another example relates to Article 27, point (c), of the draft RTS, with those NPOs pointing to	The EBA cannot grant such an exemption, as the requirements specified in the RTS have their legal basis in Article 34(4) AMLR. Granting the requested exemption in the RTS could be read as an exemption from the Level 1 requirements, which is not within the competence of the EBA. Moreover, this could lead to unintended consequences of NPOs being used as a vehicle to circumvent AML/CFT measures. Nonetheless, OEs need to apply enhanced due diligence, tailored to the risks identified and the specific circumstances of the case. This is	Inclusion of Article 1 in the RTS.

	difficulties obtaining this information, particularly those who work with partners in other parts of the world or who are operating in conflict zones or authoritarian countries.	no different for persons in vulnerable legal or economic positions. To emphasise this, the EBA explicitly included an Article 1 on proportionality and the risk-based approach.	
Article 24(a) Verification of the authenticity and accuracy of the information	Some respondents requested further clarification on the expectations pertaining to the obligation to verify the authenticity and accuracy of the additional documentation to be collected under Article 24 point (a) of the draft RTS, with one respondent proposing to use the term 'assess'.	The EBA replaced the term 'verify' in Article 25(a) of the draft RTS. Nevertheless, justified by the higher risk associated with the application of EDD measures, and in alignment with the risk-based approach, OEs should apply stricter verification methods to satisfy themselves that the (additional) information collected is authentic, accurate and reliable, to mitigate the high risk identified. The specific methods employed to achieve this are at the OEs' discretion and can include e.g. cross-checking additional information obtained from the customer with other (existing) information. The methods deployed should, in any case, be traceable.	Article 24(a) (now Article 25(a)) amended.
Article 24(b) reputation of the customer and the beneficial owners	Several respondents requested clarification on the requirement that the additional information should enable an OE to assess the reputation of the customer and the beneficial owner and whether it involves e.g. adverse media screening, information on convictions, investigations and information from credit agencies. Considering that the term *reputation* can be interpreted widely, some respondents requested the term be limited to reputation relevant for AML/CFT purposes.	The additional information OEs shall obtain to enable them to assess the reputation of the customer and the beneficial owners can include adverse media screening or similar means, information on criminal investigations, proceedings and convictions or any other relevant information, taking into account the fundamental right of the presumption of innocence. The information considered by OEs needs to be related to money laundering, its predicate offences or terrorist financing, including targeted financial sanctions, be non-discriminatory, evidence-based and available at the time of assessment. Finally, the accuracy and recency of information should also be considered in this context.	No amendments made.

Article 24(c) Customer's or beneficial owner's past and present business activities	Several respondents requested to limit the timeline for assessing the customer's or beneficial owner's past and present business activities as well as to limit it to cases of increased risk and concrete suspicion. Additionally, clarification was requested as to the nature of the information to be obtained.	The EBA deleted this separate requirement as it is covered under the current point (c) of Article 25.	Article 24(c) deleted.
Article 24(d) information on family members, persons known to be close associates or any other close business partners	Respondents flagged the possible risk of 'tipping off' and highlighted data protection concerns in case of family members, persons known to be close associates or other close business partners. Some also requested clarification on the information to be collected and documented. Respondents also emphasised the obligation to file a Suspicious Transaction Report (STR) in case of reasonable grounds to suspect criminal activity and cautioned against encroaching on areas that fall under the jurisdiction of law enforcement. Some respondents also requested the article be deleted or changed.	The EBA rephrased point (d) of former Article 24 to address concerns raised, including data protection concerns. In line with the requests from respondents, the EBA also clarified in the current Article 25, point (c), that the risk associated with any close relationships of the customer or the beneficial owners should be known to the obliged entity or publicly known, to avoid unnecessary client outreach and to address concerns over a possible violation of the prohibition of disclosure as mentioned in Article 73 of Regulation (EU) 2024/1624.	Article 24(d) (now Article 25(c) amended.
General comment Transaction and non-transaction based obliged entities	Some respondents commented that the requirements of Article 25 were too focused on transaction-based OEs and therefore less relevant for non-transaction-based OEs.	The focus of the RTS is primarily on the financial sector. Nonetheless, to ensure horizontal applicability where possible and to ensure the provisions of the RTS are suitable for a wide variety of business models used by OEs, the EBA has included a more widely applicable requirement in point (a) of current Article 26 of the RTS.	Inclusion of a new point (a) in Article 26.
Article 25(a) Destination of funds	Several respondents requested clarification on how the information should be obtained from authorities and other OEs, with one respondent asking whether they could rely on information-	The EBA revised this provision by deleting the reference to '*information from authorities and other obliged entities'* to enhance clarity and emphasise that the additional information obtained should allow the obliged entity to be satisfied that the destination of funds is consistent with the stated nature of the business relationship or occasional transaction and the customer's risk profile.	Article 25(a) (now Article 26(b) amended.

	sharing on cross-border customers for EU OEs.		
Article 25(b) expected number, size, volume and frequency of transactions that are likely to pass through the account, as well as their recipient	Some respondents requested clarification on what is expected when OEs are asked to verify the legitimacy of the expected number, size, volume and frequency of transactions. One respondent wondered whether this implies substantiating each transaction with invoices, agreements, tax statements or receipts for daily expenses such as food or utilities, citing that this would be extremely burdensome and unrealistic requirement for both customers and OEs. Another respondent requested to replace the term 'verify the legitimacy' by 'assess the plausibility'.	The EBA clarifies that the former Article 25(b) of the RTS does not impose an obligation in respect of each and every transaction, but action might be warranted in case of a deviation from the customer's transaction profile. The EBA agrees that the term *assess* is better suited in an EDD context. In addition, the EBA included 'type' of transaction, i.e. the nature or category of the transaction, and amended the language of this provision to ensure applicability to a wider variety of OEs by deleting '*transactions that are likely to pass through the account*'. Finally, the EBA emphasised, and amended accordingly, that the transactions that are expected to be performed are consistent with the declared business activity, source of funds or source of wealth of the customer.	Article 25(b) (now Article 26(c)) amended.
Article 25(c) information on the customer's key customers, contracts, business partners or associates	Some respondents requested confirmation that the obligation in this Article does not require the performance of CDD on customers clients or counterparts. Respondents also questioned how the requirements under Article 25(c) of the RTS align with obligations under the former Articles 15 and 16 of the RTS concerning the purpose and intended nature of the business relationship as there appears to be overlap.	The EBA clarifies that there is neither a requirement nor a prohibition to conduct customer due diligence on customers' clients or counterparts within an enhanced due diligence context. There may be situations where an obliged entity may consider such measures necessary, depending on the level of risk and the specific circumstances of the case. The EBA provides further clarity through the current Article 26, paragraph 2, which specifies that, for the purposes of paragraph 1, points (a) to (c), the information to be obtained by OEs may consist of additional information on the customer's key customers, contracts, business partners, associates or occasional transaction. Based on the responses, the EBA also included, *'where relevant, the beneficial owner's business partners or associates'* at the end of the current Article 26(2) of the draft RTS.	Article 25(c) (now Article 26(2)) amended.
Article 26(a), (b), (e) and (f) certification of documentation	Respondents requested clarification that 'certified' includes both physical and digital certification.	The EBA deleted the term 'certified' in the former Article 26, points(a), (b), (e) and (f), of the RTS to ensure the EDD requirements are not overly burdensome. Accordingly, the EBA simplified former point (d) and deleted former point (e). As the RTS are intended to be future proof and technologically neutral, the requirements allow for physical or digital attestation and the digitisation of CDD processes.	Article 26(a), (b), (e) and (f) (now Article 27(a), (b) and (e)) amended.

		Finally, the EBA amended Article 27(b) of the draft RTS to ensure broader applicability by including credit facility agreements.	
Article 26(g) and (h) Inclusion of any other relevant information	Some respondents asked for the inclusion of a point (h), which should read 'any other relevant information' or leave room for other sources to verify that the source of funds or source of wealth is derived from lawful activities, such as specific entities responsible for processing this type of information or other reliable open sources, e.g. public registers.	The EBA clarifies that the intention is to harmonise practices to the greatest extent possible while being mindful of the applicability of the RTS to a wide variety of OEs and situations. Therefore, the former point (g) of the RTS allowed for any other documentation to cater for information that would not match the described documentation in former points (a) to (f). To make the intention of the RTS more explicit, the EBA slightly amended the wording of the current point (h). Based on the consultation responses and subsequent discussions, the EBA also inserted a new point (g) that allows for authentic information from reputable media publications or reputable commercially available service providers, and a new point (f) on information from reliable asset or public registers to ensure flexibility and maximise meaningful outcomes. In any case, the information obtained needs to be fit for purpose.	Article 26(g) and (h) (now Article 27(f), (g) and (h)) amended.
Article 26 Clarification on source of funds and source of wealth	Respondents requested clarification on the concept of 'source of funds' (SoF) and 'source of wealth' (SoW). Respondents also requested clarification on whether SoW means that the total wealth of the customer (including assets that are not considered relevant to the customer relationship) should be covered, or whether there is a risk-based possibility for the obliged entity to concentrate the investigation on those parts of the customer wealth that pose a risk or obtain additional information on the SoW of the beneficial owner if they are linked to the customer. They cite that there may be situations where an assessment of the entire SoW of the beneficial owner becomes disproportionate and too intrusive from an integrity perspective.	The EBA clarifies that, in line with the current Article 18 of the RTS, SoF refers to the activity that generated the funds (the imitated origin) used in a transaction or involved in the business relationship. SoW is a broader concept that refers to the origin of the total wealth of the customer and of the beneficial owners. Generally, the focus is on the total wealth of the customer and the beneficial owners (e.g. how they accumulated it over time), which, in essence, applies to the full extent of the origin of their wealth, even those unrelated to the relationship with the obliged entity. The measures of Article 34(4) AMLR need to be proportionate to the higher risks identified. Therefore, the additional information to be collected on the SoW of the customer and beneficial owners is for an obliged entity to determine on a case-by-case basis, considering the risk, specific circumstances of the situation, and whether a full or partial assessment is needed to assess consistency with their overall financial position. The EBA further clarifies that Article 34 AMLR does not limit the collection of information on the SoW of beneficial owners to cases where the obliged entity has reasonable grounds to suspect criminal	No amendments made.

	Respondents also requested the article be considerate of the risk-based approach, e.g. to only require such measures in cases where there are doubts about the SoF or the SoW, or by restricting the reference to beneficial owners to cases where the obliged entity has reasonable grounds to suspect criminal activity, or limiting it to the customer unless it can be proven that the beneficial owner is contributing assets to the business relationship with the obliged entity, with some also finding the requirements for beneficial owner to be excessive.	activity or to situations where the beneficial owner contributes assets to the business relationship. Such a restrictive interpretation would undermine the effectiveness of the AML/CFT framework. Finally, while SMOs are not considered beneficial owners, as mentioned above, there may be exceptional cases where applying these provisions to SMOs is justified to mitigate the money laundering or terrorist financing risks.	
Article 27(a) verify the accuracy of the transaction's rationale	Some respondents remarked that the 'legitimacy of intended outcome' is difficult to verify, requesting clarification or deletion with some respondents requesting the EBA revise the requirement to an obligation to assess the plausibility of the transaction's justification. Another respondent remarked that the draft RTS, in their view, suggest that every transaction for high-risk customers needs to be examined to establish why it was intended.	The EBA adjusted the wording of the chapeau of the current Article 28 of the RTS, which now uses the term 'assess'. The EBA also revised point (a) to a requirement to obtain such information on which base OEs can assess the extent to which the reason provided for the transaction is credible and in line with the institution's knowledge of the customer. Finally, the current Article 28(a) of the RTS does not impose an obligation on every intended or conducted transaction but might be warranted, e.g. in case of a deviation from the customer's expected transaction profile.	Article 27(a) (now Article 28(a)) amended.
Article 27(c) assessing the legitimacy of the parties involved in the transaction	Respondents remarked that the obligation to assess the legitimacy of the parties involved in a transaction, including intermediaries and their relationship to the customer, appears to imply a requirement to conduct CDD on the customer's business partners or the recipient of a transaction. Respondents	Similar to the clarification under the current Article 28(a) of this feedback table, Article 28(c) of the RTS also does not impose an obligation on every intended or conducted transaction but might be warranted in case of a risk trigger. In addition, the EBA amended point (c) to a requirement to obtain such additional information on which basis OEs can assess the information to clarify any higher risks the obliged entity may have identified in respect of the parties involved in the transaction, including any intermediaries, in the	Article 27(c) (now Article 28(c)) amended.

	stated that this is neither feasible nor appropriate for OEs and should not be part of the EDD requirements. Other respondents requested a threshold for the transactions to be within scope of the required measures, or to ensure the requirement does not refer to every intended or performed transaction, as this will be disproportionate and lead to a disproportionate burden for OEs.	broader economic sense, and their relationship with the customer. Reliance on the presumption that the counterparty's bank has fulfilled its own customer due diligence obligations in line with EU regulations is not sufficient. Finally, the EBA clarifies that there is neither a requirement nor a prohibition to conduct customer due diligence on third parties involved in a transaction within an EDD context. There may be situations, however, where an obliged entity may deem such measures necessary, depending on the level of risk and the specific circumstances.	
Article 27(d) obtaining a deeper understanding of the customer or the beneficial owner incl. information on family members, persons known to be a close associate or any other close business partners or associates	Several respondents requested the deletion of Article 27 point (d) of the draft RTS, citing privacy issues, a risk of tipping off the customer and imprecise regulatory language, leaving too much room for varied interpretations by OEs	Based on the consultation responses, the EBA decided to delete the former Article 27(d) of the draft RTS.	Article 27(d) deleted.
Question 9 – Targeted financial sanctions (TFS)			
General comment Scope of the RTS	Respondents stated that the RTS does not introduce an obligation in the scope of applying trade or economic sanctions, where this factor would be of significant importance.	The EBA clarifies that the AMLR and RTS only cover targeted financial sanctions (one category of restrictive measures, e.g. asset freezes and prohibitions to make funds/resources available to designated persons/entities). The other category – trade or economic sanctions (e.g. arms embargoes, trade restrictions, travel bans) – is outside the scope of this framework.	Recital 20 amended.
General comment Relationship between the RTS and the EBA Guidelines on restrictive measures	Some respondents noted discrepancies between the draft RTS and the EBA/GL/2024/15 Guidelines on restrictive measures under Regulation 2023/1113 (e.g. scope of name screening, level of	According to Article 54(5) AMLAR, EBA guidelines and recommendations under Regulation (EU) 2023/1113 remain applicable until new AMLA guidelines take effect. Consequently, the EBA Guidelines on restrictive measures continue to apply. Certain provisions of the guidelines have been incorporated into the RTS,	No amendments made.

	detail on screening procedures, such as false positive management) and requested clarification on their interaction.	which, as a binding act, prevails. Overall, the draft RTS are consistent with the guidelines. Minor differences, such as the wording in current Article 30 on collecting all the first names and surnames for identification, reflect alignment with RTS requirements rather than a substantive inconsistency.	
General comment Proportionality and risk-based approach	Some respondents observed that the RTS should permit proportional and risk-based application of the controls provided for by this section.	The EBA clarifies that the current legal framework (Article 10 AMLR and EBA/GL/2024/14) already allows OEs to conduct a restrictive measures risk assessment to ensure their policies, procedures and controls match their exposure. The RTS add flexibility in how screening is performed (automatic or manual), depending on the size, business model, complexity or nature of the entity. This flexibility does not remove the binding obligation for all persons in the EU to freeze and not make funds or assets available, directly or indirectly, to designated persons or entities.	No amendments made.
Article 28 Population to be screened	Several respondents observed that the obligation to screen *all* the entities or persons which own or control the customers is too broad, as it may also include entities and persons whose identification is not legally required. Some of them suggested reducing the scope of the provisions to customers and beneficial owners.	The EBA clarifies that screening of intermediate entities for TFS must follow the criteria in Article 20(1)(d) AMLR. In this context, the notion of beneficial ownership is broader than the AMLR for the purposes of CDD, to ensure the effectiveness of TFS. Key criteria include: (1) ownership of 50% or more of an entity's proprietary rights (as explained in the 2024 EU Council Best Practices update); (2) control by means other than ownership, with examples provided in the same update; and (3) majority interest in the entity. The RTS provision has been revised to provide greater clarity.	Article 28 (now Article 29) amended.
Article 29(a) Information to be screened	Some respondents noted that there should be no obligation to include date of birth, aliases or wallet addresses in the screening itself. This information should instead be used only when a positive match occurs, to further verify whether the screened individual corresponds to the designated person. Conversely, some respondents suggested including extra data – such as addresses, wallet addresses, passport numbers,	The EBA clarifies that the information required under the current Article 30(a) aligns with what OEs must collect for CDD under Section 1 of the RTS and is generally available in TFS lists. With specific regard to the date of birth, the EBA clarified that screening of the date of birth (as well as the one on aliases and wallet addresses) is not carried out in isolation but with the screening of the first name and surname, thus limiting the number of positive hits. This information can be used at the first stage if available or later for match assessment. With regard to the second comment, the RTS specifies the minimum information needed for TFS screening of customers and entities that	Article 29a (now Article 30(a)) amended

	national IDs, or LEIs – to improve the accuracy of the screening process.	own or control them but does not prevent the use of additional information to improve screening accuracy.	
Article 29(a)(i) Transliteration of names and surnames	Respondents asked whether transliteration of names and surnames is mandatory for screening, noting that not all systems support it. Others requested clarification and consistency between the terms 'transliteration' (used in the Article) and 'transcription' (used in Recital 3) to ensure a clear understanding of the requirements.	The EBA clarifies that recording the transliteration in screening is not mandatory and should be done only if available. 'Transliteration' is the preferred term in the context of sanction screening, as it preserves the original spelling when converting characters between writing systems, whereas 'transcription' refers to converting sounds and preserving pronunciation, which is a distinct concept. To enhance clarity, the term 'transcription' has been deleted from the RTS on CDD.	Reference in Recital 3 (now Recital 2) deleted.
Article 29 (a) (iii) Screening of any other names of natural persons	Some respondents asked for clarification on what the screening of *any other names* of a natural person means.	The EBA clarifies that this term refers to alternative names not on the individual's identity document but listed in sanctions lists, ensuring that screening captures all name variations linked to a designated person.	No amendments made.
Article 29 (a) (iv) Screening of the beneficial ownership information	Several respondents noted that, under Article 62 AMLR, information on beneficial ownership for legal persons includes extensive details on beneficial owners, which could make the screening process excessively burdensome.	The EBA clarifies that not all the information listed in Article 62 AMLR must be checked for the screening itself, but only the ones listed in Article 30(a) of the RTS on CDD. The residual information can be used for assessing matches, in case of positive hits. The provision has been restructured for consistency and greater clarity on which information should be subject to screening.	Article 29 (a) (now Article 30 (a)) amended.
Article 29 (c) (iii) Significant changes that trigger the screening	Several respondents sought clarification on the notion of *significant changes*, with particular reference to changes in business operations, the occurrence of which would trigger the requirement to conduct a new TFS screening.	The EBA clarifies that new screening is required for changes in CDD data with a potential impact on designation as a listed person or entity. For example, administrative updates (e.g. contact details) do not require re-screening, whereas material changes – such as legal/commercial name, nationality, or relocation to high-risk/sanctioned jurisdictions – are considered significant and must trigger immediate re-screening. The text has been amended accordingly.	Article 29(c)(iii) (now Article 30(c)(iii)) amended.

Article 30(d) Ensuring screening without undue delay	Some respondents requested clarification regarding the obligation to ensure screening is conducted *without undue delay*.	The EBA clarifies that any time elapsed between the entry into force of a new or amended targeted financial sanction and verification of own clients should be as short as possible to ensure compliance by the OEs with their obligations under the EU Council Regulations adopted in accordance with Article 215 TFEU, which imposes the 'obligation of result' and are, in most cases, applicable on the day of their publication in the Official Journal. In this context, undue delay means 'immediately' or 'promptly', but with some allowance for operational realities (e.g. system limitations). The emphasis is on not causing unnecessary or avoidable delays.	No amendments made.
Question 10 - E-money exemptions			
Seeking clarification on the interaction between Article 19(7) AMLR and Article 30 of the draft RTS.	Respondents were seeking clarification on how to read Article 19(7) AMLR together with Article 30 of the draft RTS on CDD.	The mandate under Article 28(1) (c) AMLR explicitly allows for the RTS to specify a list of risk factors associated with features of electronic money instruments that should be taken into account by supervisors. Article 19(7) AMLR provides a list of four conditions under which an exemption from CDD measures (as otherwise required in Article (20)1(a) (b) (c)) could be granted. Deciding on whether or not to apply such exemptions remains at the national AML/CFT supervisor's discretion, as specified in Article 19(7) AMLR. The risk factors listed under Article 30 of the draft RTS will assist supervisors in making the decision on the extent of the CDD exemptions from Article 20(1), points (a), (b) and (c), AMLR.	Article 30 (now Article 31) and Recital 20 (now 21) amended.
Clarification on whether risk factors listed under Article 30 of the draft RTS should be read cumulatively	Respondents were seeking clarifications on whether risk factors listed under Article 30 of the draft RTS are cumulative or should be read one by one.	Risk factors under Article 31 of the draft RTS are not cumulative. The intention is to provide a non-exhaustive list of potential risk factors which should be considered by supervisors when deciding on the extent of exemptions from Article 20(1), points (a), (b) and (c), AMLR.	Article 30 (now Article 31) amended.
Risk factors in relation to the AML/CFT internal controls of the e-money issuers to be included in the list of risk factors	Respondents indicated that risk factors under Article 30 of the draft RTS should include factors linked to the quality of the AML/CFT controls of the issuers of the e-money instrument, subject to conditions as described under Article 19(7) AMLR.	The EBA mandate under Article 28(1), point (c), AMLR explicitly indicates that the risk factors under Article 30 of the draft RTS should focus on the 'electronic money instruments' and not on the issuers of the e-money instrument. This request is therefore outside of the scope of the EBA's mandate.	No amendments made.

	They indicated that such factors could, e.g. include distribution and/or merchant monitoring, technological safeguards, and monitoring transactions (including both purchase and redemption transactions).		
Specific weight to be attributed to the different risk factors listed under Article 30 of the draft RTS	Some respondents requested if the draft RTS provides for weight with the different risk factors as listed in Article 30 of the draft RTS – i.e. which of the listed factors can be considered sufficiently consequential when presented alone and which would be combined with others.	Article 30 of the draft RTS should be read together with Article 19(7) AMLR. Accordingly, supervisors have to apply judgement to decide whether an e-money instrument can meet the conditions of the combined reading of Article 19(7) and Article 30 of the draft RTS. Therefore, the weighing of the risk factors is not possible.	No amendments made.
Certain risk factors initially listed under Article 30 have no impact on ML/TF risks	Respondents indicated that certain risk factors, as listed in the draft RTS, may not have an impact on ML/TF risks and therefore they should be deleted from Article 31. Accordingly, they believed that the following initial elements should be deleted.	The language of the risk factors has been adjusted to give a more flexible reading. For example, the risk factors are presented by starting with 'the extent to which'. This language allowed for the risk factors, as initially identified, to be retained in Article 30.	Article 30 (now Article 31) amended.
Question 11 E-IDAS attributes			
Article 31	Some respondents requested clarification in Article 31(1) of the RTS that the use of electronic identification means is voluntary, noting that the full minimum set of attributes is not yet fully supported by Qualified Trust Services or existing EU eID schemes. Respondents also required that Article 31(2) should be deleted as it would lead to divergent approaches if additional attributes were chosen.	Electronic identities are not mandatory under the eIDAS Regulation. The EBA clarified that eIDAS tools and solutions are required by the RTS on CDD only where an eIDAS-compliant identity is available and can reasonably be expected from the customer. Where not available, OEs may rely on alternative, robust online verification methods in line with the EBA guidelines on remote onboarding. The current Article 32(2) provides OEs with flexibility to use additional attributes beyond the prescribed minimum for unambiguous identification and verification of customers or beneficial owners when justified by ML/TF risk. This ensures that due diligence can be tailored to specific situations, enhancing reliability	No amendments made.

	One respondent noted that relying solely on a qualified electronic signature (QES) under the eIDAS Regulation may not clarify which specific data points are covered. Therefore, verification via QES alone may be insufficient and should be supplemented with additional methods to verify each relevant customer identity data point.	and reducing ambiguity, rather than being limited to a fixed set of attributes under Article 22(1) AMLR. Finally, Qualified Electronic Attestation of Attributes (QEAA) is a digital attestation issued by a Qualified Trust Service Provider (QTSP) that provides trusted, machine-readable proof of verified identity attributes at a defined assurance level. Structured under Implementing Regulation (EU) 2024/2977 for integration into EDIW, a QEAA allows OEs to programmatically confirm which attributes have been verified, by whom, and at what assurance level.	
Annex	One respondent highlighted misalignment between terms in the Annex ('current legal name') and the RTS ('registered name' and 'commercial name') with no corresponding attribute in the Annex. Some respondents requested clarification on whether all attributes must be used when employing electronic identification means, and suggested removing [resident_state] as it is not currently required. They also recommended distinguishing mandatory vs optional personal identification data in the Annex to prevent optional data from becoming de facto mandatory with future business wallet use. One respondent noted the lack of guidance on capturing multiple nationalities through the attributes. Several respondents indicated that data on persons with refugee or subsidiary protection status is rarely relevant for their clients, and suggested removing this requirement due to the significant IT effort involved.	The EBA clarifies that the Annex specifies the minimum technical attributes required for customer and beneficial owner identification under Article 22(1) AMLR, drawing on Commission Implementing Regulation (EU) 2024/2977. Attributes such as 'registered name' or 'commercial name' are addressed through 'other existing attributes covering legal form', and Article 32(3) of the RTS on CDD applies where these attributes are unavailable. The Annex also ensures that all the attributes included meet the requirements for customer due diligence under Article 20(1) and 22(1) AMLR. While the Implementing Regulation distinguishes between mandatory and optional data, the RTS focus on attributes necessary for legal compliance. Nationality is represented using standard formats (e.g. ISO 3166 codes). Support for multiple nationalities depends on the issuer's system; where this is not possible, Article 32(3) of the RTS on CDD applies. Finally, the EBA clarifies that the minimum corresponding attributes in the Annex fulfil the legal obligations set out in Article 22 AMLR.	No amendments made.
Question 11 - Grace period			

Article 32 Enquiries regarding the grace period, as introduced by the RTS	Respondents enquired as to whether the transition period, as introduced by the RTS under its Article 33, would apply to the underlying AMLR, or 'only' to the RTS.	The EBA confirms that the RTS can only define its own transitional period but cannot introduce a transitional period for the underlying AMLR.	No amendments made.
Article 32 application date of the RTS	Respondents requested the EBA's clarifications on the application date of the RTS in comparison to the application date of the underlying AMLR itself.	The EBA confirms that the RTS on CDD will not be applicable earlier than the application date of the AMLR.	No amendments made.

Responses to questions relating to the RTS on pecuniary sanctions, administrative measures and periodic penalty payments (Article 53(10) AMLD6)

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Article 1 Additional indicators	Some respondents suggest additional indicators Suggestions included: -to focus more on residual risks rather than inherent risks by adding an indicator linked with data integrity and quality. - to take into account the size of the entity - to establish whether the breach was related only to the entity's own AML/CFT procedures and policies or whether it also led to the breach of the applicable regulatory obligations. - to link with the remediation measures - adding an indicator linked to the fact that the breach was committed by the entity itself or by a third party.	The impact of the breach on the ML/TF risk is covered as part of indicator under Article 1 (e). Remediation measures are taken into account as a mitigating criterion for the level of pecuniary sanctions in Article 4 (2), point b). Corrective measures are not relevant to assess the level of the gravity of a breach, but as mentioned in Article 4 (2) (b) of the draft RTS, they are to be taken into account when determining the level of pecuniary sanctions. As regards the suggestion to distinguish whether the breach was related only to the entity's policies and procedures, the entity's policies and procedures should be compliant with the regulatory obligations and be applied by the entity. Therefore, the addition of such a	No change

		distinction does not appear appropriate. The indicator mentioned in point f) refers to '*the nature of the breach by assessing the AML/CFT requirements to which the breach is related*'. If the entity is not fulfilling its obligations due to the bad quality of the data collected for CDD purpose, this would be taken into account by this indicator. Finally, the obliged entity remains responsible for its AML/CFT obligations, irrespective of any outsourcing or reliance arrangements.	
Specific metrics to indicators	Some respondents suggest adding specific metrics to the indicators listed in Article 1 (e.g. precise indications of time/numbers to the indicator linked with the duration, repetition) to ensure convergence among supervisors.	Convergence is important but setting out metrics in RTS may limit the flexibility of competent authorities to take into account the context in which the breach has occurred.	No change
Indicator (e) 'Impact of the breach on the exposure of the obliged entity'	Some respondents explained that in their view there is always an impact of the breach on exposure to the AML/CFT risk. Therefore, they wondered how this indicator e) is helpful to classify the level of gravity of a breach.	This indicator serves to measure the impact of the breach on the exposure to ML/TF risks. For instance, there could be no impact, a minor impact, a moderate impact, significant impact or very significant impact. This may be relevant also for other indicators. In this vein, Article 1 has been amended to clarify that all indicators shall be taken	Article 1(1) amended

Indicator (d) 'Impact of the breach on the obliged entity'		in consideration 'to the extent they apply'. Moreover, Article 2(2) clarifies that '*to classify the breaches in one of the four categories listed in paragraph 1, supervisors shall assess whether and to what extent all the applicable indicators of Article 1 of this Regulation are met*'.	
Indicator (g) - facilitation of criminal activities	Some respondents consider that a breach will always facilitate criminal activities or led to such criminal activities and wonder about the appropriateness of the criteria.	When assessing this criterion, supervisor will look at whether and to what extent criminal activities could have been facilitated or the breach led to such criminal activities. Article 2(2) of the draft RTS provides accordingly for every indicator set out under Article 1.	No change
Indicator (k) - systematic nature of the breach	Some respondents request further clarity on the exact meaning and differences between indicator b) 'the repetition of the breach' and indicator k) 'the systematic nature of the breach'.	Indicators b) and k) have different meanings. The 'repetition' implies a violation of the same provision a certain number of times. Article 53(6) AMLD6 distinguishes in point b) the number of instances the breach was repeated and, in point h), previous breaches by the natural or legal person held responsible. 'Systematic' implies the widespread and non-occasional nature of the breach. The breach occurs due to a certain set of methods.	No change

Indicator (h) – structural failure within the obliged entity	Some respondents request a clarification of this indicator as a 'structural banking failure' with a resolution procedure depending on a prudential analysis and falling outside of the AML/CFT supervisors' competencies	This first part of this indicator does not refer to a banking failure with a resolution procedure but specifically to a structural failure with regards to the AML/CFT systems, control and policies which fall under the AML/CFT supervisors' competencies.	No change
Indicator (j) – impact of the breach	Some respondents wonder whether this indicator means that the impact of the breach will be judged more severely for systemic financial institutions.	This indicator is assessing the actual or potential impact of the breach on the integrity, transparency and security of the financial system and the orderly functioning of the financial markets. Such an impact or potential impact is not necessarily linked to the size of an obliged entity.	No change
Article 2 Scope of the different categories defined in the RTS	Some respondents are unclear about how the different categories work and in particular whether the draft RTS give a full definition of the different categories. Some respondents wonder about the exact meaning of the sentence *'Supervisors may classify under those categories other breaches that the ones dealt with in paragraphs 4 to 6*'. Some respondents suggest that category one and two are described in too restrictive a way and that it is unlikely that breaches would fall under those categories.	The draft RTS do not give a full definition of the different categories but set out some combinations of indicators in which the breach should always be classified in certain categories in Article 2. This does not prevent supervisors from classifying other breaches in those categories. The draft RTS have been updated to make this clear. Hence category 1 and 2 are, in practice, wider.	Recital 3 and Article 2(3) amended
Minor breaches	Some respondents consider that more details should be given in the RTS to minor breaches. Some suggest that the draft RTS should say	The draft RTS do not refer to category 1 and 2 as they are not 'deemed serious, repeated or systematic in the meaning of Article 55(1) of Directive (EU)	No change

	explicitly that the lower categories (1 and 2) may warrant only minimum sanctions/that a legal effect should be attached to them.	2024/1640.' Article 55(1) AMLD6, does not prevent supervisors from imposing pecuniary sanctions for breaches that are not serious, repeated or systematic.	
Assessment of multiple breaches	Some respondents consider that the EBA should guide supervisors on how they should aggregate the indicators for further clarity, e.g. to state the conditions under which multiple breaches may be treated as a single breach for the purposes of this assessment; under which conditions the breach under category two become systematic enough for category thee.	As set out in Recital 2, when determining the level of gravity of breaches, and classifying them into the four categories, supervisors should take into account all applicable indicators and make an overall assessment of those indicators, using their supervisory judgement, to analyse whether and to what extent they are met. Supervisors can conduct an overall assessment of the gravity of different breaches, for instance when considering the findings of an inspection report.	No change
Differentiation between breaches of categories 3 and 4 and legal effect	Some respondents asked for more differentiation between breaches of categories 3 and 4, category 4 being reserved for truly egregious cases. Some respondents consider than only breaches category 4 should lead to a breach which is 'serious, repeated or systematic within the meaning of Article 55(1) of Directive (EU) 2024/1640.' and that category three may allow for more discretion in sanctioning, while still grave.	Both categories, three and four, represent a breach that should be classified as 'serious, repeated or systematic'. Moreover, according to the wording of Article 55(1) AMLD6, Member States could in any case impose pecuniary sanctions for breaches which are not serious, repeated or systematic.	No change

Isolated and unintentional incidents	Some respondents suggested that unintentional and isolated incidents should be distinguished from deliberate non-compliance.	Indicator c) takes into consideration the conduct of the obliged entity. In this regard, the RTS already underline the importance of deliberate non-compliance, in Recital 5 which states that: '(…) *Supervisors should consider whether a breach was committed intentionally or negligently. Supervisors should pay particular attention to situations where the natural person or legal person appears to have had knowledge of the breach and took no action, or where their action directly contributed to the breach.'*	No change
Article 4 Financial strength Smaller entities/ Criteria linked with the ability to pay	Respondents broadly support the inclusion of the entity's financial strength and benefit for the breach as a criterion and encourage supervisors going forward to make use of those. Some smaller firms are concerned that, in some Member States, fines have flat minimum amounts that might be crippling to them. They consider that minor breaches by a small firm should not result in disproportionate penalties. Some respondents suggest the inclusion of a criterion linked to the ability to pay without causing instability. Some respondents consider the draft RTS are not sufficiently clear on how financial strength should be taken into account in enforcement decisions while they agree it is important to consider the offender's financial strength to enhance the risk-based proportionate application of sanctions. Suggestions include:	Regarding the proportionality of the sanction, AMLD6 provides that Member States shall 'i*mpose effective, dissuasive and proportionate pecuniary sanctions*'. In the same vein, Article 53(2) AMLD6 states that '*Any sanction imposed or measure applied pursuant to this Section shall be effective, proportionate and dissuasive*'. Therefore, the application of criteria set out in the draft RTS should comply with such principles. With regard the ability to pay, Article 55(5) AMLD6 indicates that "*Member States shall ensure that, when determining the amount of the pecuniary sanction, the ability of the*	Article 4(5) and 4 (6) amended

- the fact of using it as a proportionality tool;
- the fact of referring to the financial ratio analysis (such as current ratio, debt-to-asset ratio, interest coverage ratio, etc.):
- information on Profitability. Liquidity and Capital adequacy;
- the entity's ML/TF risk exposure and potential impact on the market
- the investment made to ensure AML/CFT compliance:

With regard to natural persons, some respondents suggest taking in consideration:

- Whether the natural person derives indirect financial benefit from ownership or control of legal entities involved in the breach, including income deriving from the breach
- The degree to which their personal assets are intertwined with corporate structures
- Whether the income is deriving from the entity in which the breach is committed or from other entities

obliged entity to pay the sanction is taken into account'. Accordingly, that principle shall apply and consequently the addition of a dedicated criterion does not appear necessary.

Financial strength should be considered from a proportionality perspective, in order to determine, on a case-by-case analysis and in conjunction with the other criteria, the appropriate level of the pecuniary sanctions. In this regard, the ability to pay the sanction and the impact on the prudential requirement are already considered under Article 55(5) AMLD6. Additionally, the general principle of proportionality applies to the sanctioning and enforcement activity and thus no further amendments are needed in this regard.

With regards to the proposals put forward by the respondents, those related to the entity's ML/TF risk exposure, potential impact on the market and investments on AML/CTF compliance are not strictly connected to financial strength and cannot be considered accordingly.

With regards to the information on financial ratio analysis related to

		profitability, liquidity and capital adequacy, Article 4(5) of the draft RTS already takes into consideration the '*information from the financial statements and information from prudential authorities on the level of regulatory capital and liquidity requirements*'. Moreover, such indicators do not always apply to all obliged entities. The text has been amended to provide more details in this regard. With regard to natural persons and the comments related to the benefit deriving from the breach, this is already considered as an aggravating criterion under Article 4(3), point (d) of the RTS. The text provides for more details with specific regard to natural persons and clarifies that the assessment shall be made on information made available.	
Risk of loss caused to customer or other market users	Some respondents consider that the 'risk of loss caused to customer or other market users' in Article 4 3) (e) is too broad as a criterion as there is always a risk of loss caused to customers	When assessing the criteria, the supervisors should take into account all applicable criteria and make an overall assessment of those criteria using their supervisory judgement, as set out in Recital 2 of the draft RTS. In this regard, the risk of loss to customers, or other market users is coherent with the risk-	No change

		oriented nature of the AML/CFT legislation, and it will be considered when it is significant.	
Remediation and good intent Suggestion of additional criteria for the mitigation of the breach	Article 4(2) lists mitigating factors such as quickly ending the breach. Respondents welcome this, noting that it encourages a prompt culture of remediation. A few respondents suggested adding, as a mitigating criteria: -the proactive self-report of an issue to the supervisor -the significant investment of the entity in compliance improvement after a breach - the fact that relevant preventive AML/CFT measures were in place: some suggest also acknowledging if the firm played a positive role in broader AML initiative as context in information sharing partnerships, although some recognise it is more nebulous and probably outside of the scope of the RTS The residual ML/TF risk associated with the breach	- Proactive self-reporting is already covered in Article 4 (2) '(*a) 'has quickly and effectively brought the complete breach to the supervisor's attention'.* - Regarding the '*fact that relevant preventive AML/CFT measures were in place*', this cannot be considered as a mitigating factor *per se*, as it as it merely entails compliance with AML/CFT provisions. As regards the '*significant investment of the entity in compliance improvement after a breach*' Article 4 (2) (b) the effective remediation is covered in Article 4(2) (b) '*whether the natural or legal person held responsible has taken effective and timely remedial actions to end the breach or has taken voluntary adequate measures to effectively prevent similar breaches in the future*' - With regards to the comments related to partnerships, taking part in partnership does not exclude nor reduce per se the responsibility of the	No change

		obliged entity and thus cannot be considered as a mitigating criterion. - With regards to the comments related to the 'm*agnitude of residual risk associated with the breach*' (criterion 3) b) that the conduct and the remedial actions of the obliged entity be indirectly taken into consideration.	
Prior violation and repeated conduct	This criterion was generally supported by the industry. A few responses suggested that the RTS could specify a time horizon concerning past breaches (e.g.: 5 years) and/or whether past minor breaches should count against an entity if handled adequately at that time. They mention that further guidance would be useful.	The draft has been amended to make clear that what matters are the previous breaches by the natural or the legal person held responsible and whether the supervisor has imposed any previous sanction concerning an AML/CFT breach.	Article 4(3) amended
Natural or legal person held responsible	This criterion is broadly supported by participants in particular the fact that supervisors should consider the functions and role of individuals when sanctioning. They agree that a compliance officer who lacks resources is a different case than a senior manager who willfully ignored signals. Some respondents consider that supervisors should use this criterion to ensure fine are applied to culpable decision makers and not to those who have not been supported or have been overruled. One respondent suggested explicitly adding the proactive attempt of a manager to escalate issues as a mitigating element. Some respondents also commented that the responsibility of natural person should be limited to cases where it may be demonstrated that the	Criteria under Article 4 (2), point (a) and 4(2) point (b) are sufficiently broad to consider all the activities carried out by the natural person held responsible to end the breach or the prevent similar breaches in the future. Regarding the suggestion related to a possible limitation of the responsibility of natural persons, the obligations of natural persons are defined by the AML/CFT package and relevant national transposition provisions, and that they	No change

	individual conduct of such natural persons had a direct impact on the identified / sanctioned breach.	fall outside the scope of the present RTS.	
Natural person who are not themselves obliged entities	Some respondents considered that the concept of '*natural persons which are not themselves obliged entities*' would merit clarifications and be limited to natural persons who are in a decision-making capacity affecting the actual ML/TF risk of obliged entities. Some respondents considered that the draft RTS should clarify the legal conditions for imposing pecuniary sanctions to such individuals in order to better serve the principle of legality and ensure convergence in supervisory practices.	The concept of '*natural persons which are not themselves obliged entities*', includes all natural persons that, under AMLD6 and relevant national transposition provisions, can be addressed with administrative or sanctioning proceedings. Accordingly, the definition of the legal condition for applying administrative measures or imposing pecuniary sanctions to such individuals is set out in the level 1 provision and fall outside the mandate of the RTS.	No change
Article 5 Suggestion for additional criteria for the most severe measures	-Limitation or restriction of business: some respondents considered that this should apply when specific lines of business or areas of operation pose high ML/TF risks or have serious compliance failing- -Withdrawal of authorisation: respondents considered that this measure should be used as a last resort measure only for the more severe situations with the highest level of gravity -Change in governance structure: some respondents underline the change would be appropriate in cases where AML/CFT failures stem from poor leadership or oversight. Some other respondents suggest elements to be considered when requiring changes in the governance structure, such as evidence of	To promote convergence of practices among Member States, the draft RTS focuses on the measures with the highest potential impact on the obliged entities, as underlined in Recital 5. Such an approach explains the reference to category 3 and 4 of the breach. Article 4 does not set forth an automatic mechanism for the application of the administrative measure but provides criteria that shall be taken into account by the competent authorities when considering applying those measures.	*No change*

governance failure that has led to material AML/CFT breaches, lack of internal controls or conflicts of interests. In general, some responses consider those measures should fit into an escalation ladder to give the institution a chance to correct issues before harsher steps are taken: -Some considered that the RTS should provide more guidance on when to escalate - Some respondents suggested the application of the most severe measure, such as the withdrawal of the authorisation, should be taken in consideration only after the failure of a dedicated remedial plan presented by the supervised entity - The effect on the institution's stability and on customers should be carefully assessed when applying extreme measures -Some respondents considered the RTS should contain more granular scenarios for the RTS to be more predictable, transparent and fair. -Some considered that they should not be related to 'potential breach' but only to an effective breach, and/or that that the measure listed in the RTS should be limited to category 4 breaches.	As set out in Recital 2 of the draft RTS and Article 53(6) AMLD6 such assessment shall be comprehensive of all the circumstances of the case and carried out in the light of the principle of proportionality, in order to identify the most appropriate measure to tackle the shortcomings and restore compliance. As regards the limitation or restriction of business, criteria 2)(b) and (c) assess the impact or potential impact of the breach as well the extent to which the business, operations or network are affected. As regards the change in governance structure, and the request to use it in the case of poor leadership or oversight, it must be noted that the RTS refers to the conduct of the natural or legal person held responsible in Article 5 (4) (b). As regards the withdrawal of authorisation, it is indeed the most severe measures listed in Article 5 of the draft RTS. In line with the principle of proportionality, it should be considered as a measure to address the most serious cases. However, since such

		a measure aims to restore compliance in the market, it cannot be dependent on the prior failure of a dedicated remedial plan presented by the supervised entity. The same reasoning applies to the other measure mentioned in the article. With regards to the suggestion to provide more granularity, the draft RTS aim to provide sufficient balance between the need for convergence of practices and for sufficient flexibility enabling supervisors to take into account the specific context in which the breach has occurred, as explained in Recital 2 of the draft RTS. Regarding the mention of 'potential breach', Article 56(1)(b) AMLD6 provides that administrative measures can also be applied in order to prevent the occurrence of serious, repeated and systematic breaches or reduce the risk thereof.	
Assessment of any other information in Article 5(e)	Some respondents consider it reasonable that information in Article 5(e) are considered but stressed that such information should be used in a consistent way and ensure firms can respond to it.	According to Recital 88 AMLD6, supervisors should ensure transparency with respect to the supervisory activities they have carried out, such as pecuniary sanctions imposed or	No change

		administrative measures applied. The right of defence applies.	
Coordination with other criminal prosecutors/other supervisors	Some respondents underlined that, in their view, cooperation with criminal prosecutors and other authorities is key to avoiding unintended fallouts or double punishment	Defining the rules for cooperation is not within the scope of these RTS but the principles governing to cooperation between the different authorities are envisaged under Chapter V AMLD6.	No change
Criteria related to natural persons	Most respondents are in favour of greater clarity and details when it comes to natural persons. Specific attention is given to senior management, who are not classified as obliged entities but hold key decision-making roles. Greater specificity would, in the respondents' view, enhance both deterrence and legitimacy of enforcement, ensuring individuals are sanctioned in a way that reflects their true influence on the compliance environment. According to some respondents, criteria and indicators should take into consideration the type of involvement and the nature of responsibilities held by the legal person. Some comments suggest introducing other aggravating criteria such as: - Wilful blindness, failure to act despite red flags or encouragement or tolerance of non-compliances Or mitigating criteria, such as: - The proactive approach to AML/CFT compliance or whether the individual has acted with integrity and transparency in dealing with supervisors;	The proposal related to the activities carried out by the person involved after the breach and the wilfulness of the conduct can be considered as a specification of the indicator provided under Article 1(c), that takes into consideration the conduct of the legal person that led or permitted the breach, and criteria set out under Articles 4(2)(b) and 4(3)(b), which consider the conduct of the natural person since the breach was identified. In the same vein, the level of cooperation is considered under Articles 4(1)(a) and 4(2)(b). Accordingly, the above indicator and criteria are sufficiently broad to include the main part of suggestions received in this regard. To meet the demand for greater detail when assessing the level of a pecuniary	Article 4(4) amended

	- Documented, good faith action to raise concerns, promote improvements or escalate issues, especially in the face of internal resistance. Other comments go in the direction of specifying the types of measures that can be imposed on natural persons who are not obliged entities and clarifying the definition and threshold of liability of senior managers.	sanction against natural persons, the text has been amended. With regard to the further specifications required (i.e: type of measure to be imposed on natural persons, definition and threshold of liability), such issues fall under AMLD6 and national implementation law, and thus fall outside the scope of the draft RTS.	
Article 7 time limit for the submission of written statement	Some respondents would in favour of the draft RTS stipulating conditions under which the time limit for the submission of the written statement by the obliged entity could be extended. One respondent proposed deleting Article 7 as this respondent argued that procedural questions should be governed by national law only.	The draft RTS are clear that as long the provisions of the RTS do not stipulate otherwise, the provisions of national administrative law apply. The wording of Article 6(1) of the draft RTS provides for the use of the administrative procedure as stipulated by national law. For this reason, the conditions under which the submission of written statements by the obliged entity can be extended are part of national legislation.	
Article 8 Granularity of factors needed for the calculation of PePPs	The majority of respondents are in favour of more granular rules when it comes to factors that are taken into consideration for the purpose of calculation of PePPs. Suggestions include, for example, the duration of the breach, the reputational impact and systemic impact.	PePPs should not be regarded as a sanction, but as an enforcement measure that aims to ensure that the obliged entity returns to compliance with its duties as envisaged by the administrative measure. In order to avoid the use of the same factors that led to the imposition of the administrative measure, the	No change

		draft RTS focus on factors to be used if the obliged entity does not comply with the decision on the imposition of the administrative measure.	
Article 9 More specific rules on the calculation of PePPs	The majority of the respondents are of the view that the draft RTS should include some of the following rules when it comes to the calculation of the amount of the PePP. Specifically, the respondents propose including provisions on: - reducing the amount of the penalty; - dynamic adjustments based on evidence of residual risk; - progressive scale or an exemption for entities demonstrating compliance efforts; - establishing a quantifiable baseline amount – baseline daily penalty; - defining aggravating and mitigating factors; - maximum and minimum penalty ranges; - calculation formulas linked to entity size and gravity of breach; - recognising rapid remediation capabilities; - including standards for automated compliance systems, recognition of digital audit trails, support for technology-enabled remediation, assessing digital controls.	Cases for which administrative measure are imposed can be very specific and thus there is a need for a framework that is flexible. The majority of provisions proposed by respondents focused on the underlying breach which led to the imposition of the administrative measure in question, which is not the aim of the PePP. The AML/CFT framework allows the competent authority to take the necessary steps if the obliged entity does not comply with the imposed administrative measure. These steps include, but are not limited to, PePPs.	No change
Calculation of PePP – daily, weekly, monthly basis	Some respondents would welcome more rules that would stipulate when PePPs should be calculated on a daily, weekly or monthly basis.	The draft reflects that the applicable administrative law in some Member States already allows the calculation of PePPs on a daily, weekly or monthly basis. The provision	No change

		in question allows that this principle is also used for the future, and that AML/CFT supervisors may remain flexible in how to address the specificities of the circumstances of the breach of an applicable administrative measure that has not been complied with.	
Article 10 Limitation period	Some respondents would favour more clarity about the limitation period.	Article 10 of the draft RTS covers limitation period for collecting PePPs. This article is not about time limits for how long an AML/CFT supervisor may impose the payment of a PePP, which is included in Article 57(4) AMLD6.	No change
Additional provisions when it comes to administrative procedure	A respondent would favour of the draft RTS containing: - timelines for payments and appeals; - right of representation and appeal; - methods of appeal; - taxonomy for breach categories; - interrupting the enforcement during appeal period; - rules on enforcement; - rules to ensure prevention of double sanctioning under administrative and criminal frameworks or under specific laws for the non-financial sector and general administrative law; - rules on remediation, reporting and transparency; - publication of periodic penalty decisions;	The provisions on PePP contained in the draft RTS focus only on specific rules concerning the administrative procedure. Most of the provisions proposed by the respondents are governed by national administrative law. As the mandate included in Article 53(10) AMLD6 targets the imposition of PePPs for the breach of some types of administrative measures and not for all of them, the set-up of a complex framework of administrative rules for the imposition of PePPs under the current wording of the AMLD6 would lead to the application of different procedures at national level, where the majority of enforcement	No change

	- conditions to waive, reduce or defer payments; - extending the right to be heard to the whole RTS, not only to PePPs; -procedural deadlines for supervisory processes e.g. sending the statement of findings to the supervisor.	measures would be governed only by national provisions of administrative law and a small number of cases would be governed by a different type of administrative rules. Thus, when it comes to the imposition of PePPs, the draft RTS refer to the application of national provisions of administrative procedures unless the RTS stipulate otherwise. The mandate contained in Article 53(10)(c) AMLD6 covers methodology for the imposition of PePPs, but not methodology for the imposition of pecuniary sanctions and administrative measures. As for rules concerning publication and transparency, such rules are contained in Articles 58, 59 AMLD6, which will be transposed into national legislation. For this reason, such rules cannot be included in the draft RTS.	

5. Annexes

Annex 1 - Data Points to be collected for the purpose of the RTS under Article 40(2) AMLD6 and Article 12(7) AMLAR.

Section A – Inherent risk

(1) The data points in this annex are not the same as the indicators supervisors will use to calculate the ML/TF risk of each financial institution.

			Sectors (Please refer to the interpretive note)									
Risk Category	**Sub-Category**	**Data points**	**CI**	**CP**	**LI**	**EMI**	**PI**	**BC**	**IF**	**AMC**	**CASP**	**O**
Customers	**Customers**	**Total number of customers**	x	x	x	x	x	x	x	x	x	x
		Number of customers which are Natural Persons (NP) per country	x	x	x	x	x	x	x	x	x	x
		Number of customers which are Legal Entities (LE) per country	x	x	x	x	x	x	x	x	x	x
		Number of customers NP who are PEPs per country	x	x	x	x	x	x	x	x	x	x
		Number of customers LE whose UBO are PEPs per country	x	x	x	x	x	x	x	x	x	x
		Number of customers with at least one transaction in the previous year	x	x		x	x	x	x	x	x	x
		Number of new customers in the previous year	x	x	x	x	x	x	x	x	x	x
		Number of legal entities with complex corporate structure	x	x	x	x	x		x	x	x	x
		Number of customers with high risk activities	x	x	x	x	x	x	x	x	x	x
		Number of legal entities with at least 1 UBOs located in non-EEA countries (residence)	x	x	x	x	x		x	x	x	x
		Number of customers with cross border transactions involving non-EEA countries	x	x	x	x	x	x	x	x	x	x
		Number of walk-in customers	x			x	x	x			x	
		Number of occasional transactions carried by walk in customers	x			x	x	x			x	
		Number of customers with requests from FIU	x	x	x	x	x	x	x	x	x	x
Products	**Payment Accounts**	**Number of payment accounts**	x	x		x	x					x
		Total Value (EUR) of incoming transactions in the previous year	x	x		x	x					x
		Number of incoming transactions in the previous year	x	x		x	x					x
		Total Value (EUR) of outgoing transactions in the previous year	x	x		x	x					x
		Number of outgoing transactions in the previous year	x	x		x	x					x
		Total Number of master accounts with linked vIBANS	x			x	x					

			Sectors (Please refer to the interpretive note)									
Risk Category	Sub-Category	Data points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
	Virtual IBANs	Number of transactions on Virtual IBANs (incoming) in the previous year	x			x	x					
		Total Value (EUR) of transactions on Virtual IBANs (incoming) in the previous year	x			x	x					
		Number of transactions on Virtual IBANs (outgoing) in the previous year	x			x	x					
		Total Value (EUR) of transactions on Virtual IBANs (outgoing) in the previous year	x			x	x					
		Total Number of re-issued IBANs	x			x	x					
		Total Number of re-issued IBANs where the end-user is not a customer of the obliged entity	x			x	x					
	Prepaid Cards	Total Number of Prepaid Cards issued during the previous year	x			x	x				x	
		Total Value (EUR) of the issued prepaid cards during the previous year (turnover)	x			x	x				x	
		Total Value (EUR) outstanding on prepaid cards issued during the previous year (turnover)	x			x	x				x	
		Total number of customers using prepaid cards	x			x	x				x	
		Total number of customers using prepaid cards with more than 3 prepaid cards	x			x	x				x	
	Lending	Total Number of outstanding loans	x	x								
		Total Value (EUR) of outstanding loans	x	x								
		Total Number of outstanding real estate loans	x	x								
		Total Number of outstanding real estate loans with third party payments in the past calendar year	x	x								
		Total Value (EUR) of loans granted during the previous year	x	x								
		Total Number of outstanding asset backed loans with cash collateral	x	x								
		Total Number of loan repayments during the previous year	x	x								
		Total Number of prematurely repaid loans during the previous year	x	x								
		Total Number of loan repayments from non-EEA countries during the previous year	x	x								
		Total Number of consumer loans granted during the previous year that are not associated to the acquisition of any product/service	x	x								

			Sectors (Please refer to the interpretive note)									
Risk Category	Sub-Category	Data points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
	Factoring	Total Number of factoring contracts granted in the previous year	x	x								
		Total Value (EUR) of factoring contracts granted during the previous year	x	x								
		Total Value (EUR) of factoring contracts granted to obligors established in non-EEA countries during the previous year	x	x								
	Life insurance contracts	total amount (EUR) of gross written premiums in the previous year (incoming)			x							
		total of amount (EUR) of surrender value of the insurance contracts at the end of the previous year			x							
		% of all gross written premium (amount in EUR) paid directly to the life insurance broker in the previous year			x							
		Number of insurance contracts that are not used for low risk contracts			x							
	Currency Exchange (involving cash)	Number of currency exchange transactions carried out during the previous year (sell)	x			x	x	x				
		Number of currency exchange transactions carried out during the previous year (buy)	x			x	x	x				
		Number of currency exchange transactions carried out during the previous year, where the transaction is above EUR 1 000 (sell)	x			x	x	x				
		Number of currency exchange transactions carried out during the previous year, where the transaction is above EUR 1 000 (buy)	x			x	x	x				
		Total Value (EUR) of currency exchange transactions carried out during the previous year (sell)	x			x	x	x				
		Total Value (EUR) of currency exchange transactions carried out during the previous year (buy)	x			x	x	x				
		Value (EUR) of currency exchange transactions cash-to-cash carried out during the previous year	x			x	x	x				
	Custody of crypto assets	Number of customers owning crypto-assets	x			x	x				x	
		Total value (EUR) of crypto assets held on customer custody wallets in the previous year	x			x	x				x	
Services	Invest. Services	number of retail clients	x						x	x		
		number of professional clients	x						x	x		

			Sectors (Please refer to the interpretive note)									
Risk Category	Sub-Category	Data points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
	and Activities - reception and transmission of orders	Number of AML/CFT regulated customers outside the EEA	x						x	x		
	Invest. Services and Activities - custody account keeping	number of retail clients	x						x			
		number of professional clients	x						x			
		% of assets under custody for which the obliged entity does not have a direct business relationship with the final investor	x						x			
		Number of AML/CFT regulated customers outside the EEA	x						x			
	Invest. Services and Activities - Portfolio manang ement	number of retail clients	x						x	x		
		number of professional clients	x						x	x		
		total assets under management	x						x	x		
		Number of customers for which customer holding total assets with a value of at least EUR 5 000 000	x						x	x		
	Money Remittance	Total Number of money remittance payments in the previous year (incoming)	x			x	x					
		Total Number of money remittance payments in the previous year (outgoing)	x			x	x					
		Total Value (EUR) of remittance payments in the previous year (incoming)	x			x	x					
		Total Value (EUR) of remittance payments in the previous year (outgoing)	x			x	x					
		Total Number of money remittance transactions above 1 000 euro in the previous year (incoming)	x			x	x					
		Total Number of money remittance transactions above 1 000 euro in the previous year (outgoing)	x			x	x					
	Wealth Management	Total Number of customers (NP) with total assets under management over a value of at least EUR 5 000 000 AND with total assets over a value of at least EUR 50 000 000	x		x				x		x	
		Total Number of customers (NP) that fall under the definition of private banking (EBA Risk Factor Guidelines)	x		x				x		x	
		Total Value (EUR) of transactions executed on behalf of the	x				x				x	

			Sectors (Please refer to the interpretive note)									
Risk Category	Sub-Category	Data points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
	Correspondent services	respondent client in the previous year (incoming)										
		Total Value (EUR) of transactions executed on behalf of the respondent client in the previous year (outgoing)	x				x				x	
		Total Value (EUR) of transactions going through payable through accounts in the previous year (incoming)	x				x				x	
		Total Value (EUR) of transactions going through payable through accounts in the previous year (outgoing)	x				x				x	
		Total Value (EUR) of transactions going trough nested accounts in the previous year (incoming)	x				x				x	
		Total Value (EUR) of transactions going trough nested accounts in the previous year (outgoing)	x				x				x	
	Trade finance	Total Number of trade finance customers	x	x								
		Total Number of trade finance transactions in the previous year (incoming)	x	x								
		Total Number of trade finance transactions in the previous year (outgoing)	x	x								
		Total Value (EUR) of trade finance transactions in the previous year (incoming)	x	x								
		Total Value (EUR) of trade finance transactions in the previous year (outgoing)	x	x								
	E-Money	Number of e-money payment transactions in the previous year (incoming)	x			x						
		Number of e-money payment transactions in the previous year (outgoing)	x			x						
		Total Value (EUR) of e-money payment transactions in the previous year (incoming)	x			x						
		Total Value (EUR) of e-money payment transactions in the previous year (outgoing)	x			x						
		Value (EUR) of e-money payment transactions by non-identified customers in the previous year	x			x						
	TCSP services	Total Number of legal entity customers using TCSP services in the previous year	x						x			
	Crypto cash cards	Number of non-EEA crypto companies for which the obliged entity acts as a BIN-sponsor	x			x	x					
	Exchange crypto for funds	Total amount (EUR) crypto-funds in the previous year	x			x	x		x		x	
		Total number of transactions crypto-funds in the previous year	x			x	x		x		x	

			Sectors (Please refer to the interpretive note)									
Risk Category	Sub-Category	Data points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
		number of customers using this type of service in the previous year	x			x	x		x		x	
		Total number of transactions crypto-funds from unhosted wallets in the previous year	x			x	x		x		x	
	Exchange funds for crypto	Total amount (EUR) funds-crypto in the previous year	x			x	x		x		x	
		Total number of transactions funds-crypto in the previous year	x			x	x		x		x	
		number of customers using this type of service in the previous year	x			x	x		x		x	
		Total number of transactions funds-crypto to unhosted wallets in the previous year	x			x	x		x		x	
	Exchange crypto for crypto	Total amount (EUR) crypto-crypto in the previous year	x			x	x		x		x	
		Number of customers using this type of service in the previous year	x			x	x		x		x	
		Total number of transactions crypto-crypto in the previous year	x			x	x		x		x	
		Total number of transactions crypto-crypto to unhosted wallets in the previous year	x			x	x		x		x	
		Total number of transactions crypto-crypto from unhosted wallets in the previous year	x			x	x		x		x	
	Transfer crypto-assets	Total amount (EUR) that customers transferred in the previous year	x			x	x		x		x	
		Number of customers using this type of service in the previous year	x			x	x		x		x	
		Total number of transfers of crypto-assets in the previous year	x			x	x		x		x	
		Total number of transactions to unhosted wallets in the previous year	x			x	x		x		x	
		Total number of transactions from unhosted wallets in the previous year	x			x	x		x		x	
	Management of UCITS	Number of retail investor customers								x		
		Number of professional investor customers								x		
		Total assets under management of UCITSs								x		
	Management of AIFs	Number of retail investor customers								x		
		Number of professional investor customers								x		
		Number of open-ended funds								x		
		Number of closed-ended funds								x		
		Total assets under management								x		
		Total assets under management in unlisted assets								x		

			Sectors (Please refer to the interpretive note)									
Risk Category	Sub-Category	Data points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
	Safe Custody Services	Total Number of customers using safe deposit boxes	x									
	Crowdfunding	Total Value (EUR) of funding projects in the previous year	x	x		x	x		x		x	
		Total Number of projects being funded in the previous year	x	x		x	x		x		x	
		Total Number of donors from high-risk countries	x	x		x	x		x		x	
		Total Number of projects where the owner is from a high-risk country	x	x		x	x		x		x	
	Cash Transactions	Number of cash transactions in the previous year (withdrawals)	x	x	x	x	x				x	
		Number of cash transactions in the previous year (deposits)	x	x	x	x	x				x	
		Total Value (EUR) of cash transactions in the previous year (withdrawals)	x	x	x	x	x				x	
		Total Value (EUR) of cash transactions in the previous year (deposits)	x	x	x	x	x				x	
		Total Number of natural persons totalling cash transactions over 20 000 EUR during the previous year	x	x	x	x	x				x	
Geographies	Geographies	Number of incoming transactions in the previous year by country	x	x	x	x	x	x			x	x
		Total value (EUR) of incoming transactions in the previous year by country	x	x	x	x	x	x			x	x
		Number of outgoing transactions in the previous year by country	x	x	x	x	x	x			x	x
		Total value (EUR) of outgoing transactions in the previous year by country	x	x	x	x	x	x			x	x
		Total value (EUR) of entity's investment undertakings (CIUs) by country								x		
		Number of investors by country							x	x		
		Total value (EUR) of assets under management by country								x		
		Number of institutions established in foreign countries to whom you provide correspondent services (by country)	x				x				x	
		Total value of incoming funds moved on behalf of the respondent's clients by country of respondent's establishment	x				x				x	
		Total value of outgoing funds moved on behalf of the respondent's clients by country of respondent's establishment	x				x				x	
		Number of branches by country	x	x	x	x	x	x	x	x	x	x

			Sectors (Please refer to the interpretive note)									
Risk Category	**Sub-Category**	**Data points**	**CI**	**CP**	**LI**	**EMI**	**PI**	**BC**	**IF**	**AMC**	**CASP**	**O**
		Number of subsidiaries by country	x	x	x	x	x	x	x	x	x	x
		Country where the entities undertaking is located (parent company)	x	x	x	x	x	x	x	x	x	x
Distribution channels	**Distribution channels**	**Number of new customers onboarded remotely in the previous year**	x	x	x	x	x				x	x
		Number of new customers onboarded in the previous year by third parties	x	x	x	x	x				x	x
		Number of customers onboarded in the previous year by third parties not directly subject to AML/CFT supervision	x	x	x	x	x				x	x
		Number of agents by country				x	x		x			
		Number of distributors by country				x						
		Total value of gross written premiums through insurance contracts issued through brokers, broken down by country the brokers are established			x							
		Number of white labelling partners by country of establishment	x			x	x				x	x

Section B – AML/CFT Controls

Category	Data Points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
1 - Governance, Culture & Compliance function (Role and responsibilities of the management body, AML/CFT risk culture, AML/CFT Compliance Function and Resources, AML/CFT training)	Date at which the procedures covering the entirety of the AML/CFT framework (including initial and ongoing CDD, transaction and business relationship monitoring, STR, and financial sanction screening) were checked as being in compliance with existing laws and regulations applicable at that date	x	x	x	x	x	x	x	x	x	x
	Number of dedicated AML/CFT compliance staff (in FTE)	x	x	x	x	x	x	x	x	x	x
	% of personnel per category who have received AML training during the last calendar year: a) AML/CFT compliance staff b) non-AML/CFT compliance staff (e.g. customer facing staff) c) agents and distributors d) Board members / non-executive directors	x	x	x	x	x	x	x	x	x	x
2 - Internal Controls & Outsourcing (Internal controls and reporting systems, Outsourcing	Frequency of reporting by the AML compliance officer to the management body (never, monthly, quarterly, half-yearly, yearly)	x	x	x	x	x	x	x	x	x	x

Category	Data Points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
and reliance on third parties, Internal audit function / external expert, Record keeping)	Tasks outsourced by the obliged entity (in total or in part) to service providers: CDD Training Transaction Monitoring Suspicious Transaction Reports Sanctions Screening PEP detection Compliance Monitoring Checks	x	x	x	x	x	x	x	x	x	x
	AML/CFT tasks outsourced to an external service provider located in third country that is not part of the group (Y/N)	x	x	x	x	x	x	x	x	x	x
	Existence of AML/CFT tasks outsourced to an external service provider located in third country that is part of the group (Y/N)	x	x	x	x	x	x	x	x	x	x
	Dates when the AML/CFT obligations/ controls were last assessed by an internal/external audit: a. BWRA b. determination of ML/TF risk profile of customers in a business relationship c. AML/CFT-related awareness-raising and staff training measures d. Identification and identity verification procedures e. Policies and procedures for monitoring and analysing business relationships, including transaction monitoring f. Policies and procedures for suspicious transaction reporting g. Record keeping policies and procedures h. Resources dedicated to AML/CFT i. Organisation of the AML/CFT system, governance and reporting to management bodies.	x	x	x	x	x	x	x	x	x	x
3 - Risk assessment (Business Wide Risk Assessment (BWRA) and Customer ML/TF risk assessment and classification (CRA))	Last approval date of the BWRA	x	x	x	x	x	x	x	x	x	x
	Senior management approved the last version of the BWRA (Y/N)	x	x	x	x	x	x	x	x	x	x
	Date of the last update of the CRA	x	x	x	x	x	x	x	x	x	x
	Number of customers per ML/TF risk category (low risk, medium-low risk, medium-high risk, high-risk)	x	x	x	x	x	x	x	x	x	x
4 - Customer due diligence & monitoring (Customer Due Diligence and Ongoing monitoring of business relationships)	Number of customers that are legal entities /trusts whose beneficial owners have not been identified	x	x	x	x	x	x	x	x	x	x
	Number of customers that are legal entities /trusts whose beneficial ownership has been identified, but the identity of whom has not been verified	x	x	x	x	x	x	x	x	x	x
	Number of customers without identification and verification documentation/ information	x	x	x	x	x	x	x	x	x	x
	Number of customers whose CDD data and information is not yet in line with the requirements of Article 20 AMLR	x	x	x	x	x	x	x	x	x	x

Category	Data Points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
	Number of customers without ML/TF risk profile (excluding customers with whom the obliged entity does not have a business relationship)	x	x	x	x	x	x	x	x	x	x
	Number of customers for whom updates of customer information were due in the last calendar year, in accordance with the obliged entity's policies and procedures	x	x	x	x	x	x	x	x	x	x
	Number of customers for whom customer information was reviewed and updated in the last calendar year	x	x	x	x	x	x	x	x	x	x
5 - Transaction monitoring and Suspicious Activity Reporting	The obliged entity has a transaction monitoring system in place (Y/N)	x	x	x	x	x	x	x	x	x	x
	The transaction monitoring system is: a) Not automated; or b) At least partly automated	x	x	x	x	x	x	x	x	x	x
	If manual system: Average time in days to analyse the transaction since the moment it occurred	x	x	x	x	x	x	x	x	x	x
	If automated system: The system can generate alerts in case of inconsistencies between CDD information relating to the customer and the following elements: a) Number of transactions b) Value of aggregated transactions c) value of single transactions d) counterparties e) countries	x	x	x	x	x	x	x	x	x	x
	If automated system: Number of alerts not analysed at the end of the calendar year	x	x	x	x	x	x	x	x	x	x
	If automated system: Average time to analyse an alert in the last calendar year (number of days between that the alert was generated and the moment that the alert was closed)	x	x	x	x	x	x	x	x	x	x
	If automated system: Ratio between number of alerts and number of STRs	x	x	x	x	x	x	x	x	x	x
	The entity has implemented a tool that enables it to analyse the information available on distributed ledgers and generate alerts where unusual patterns or risk factors are identified, in relation to the transactions carried out by the customer (Y/N)	x			x	x		X		x	
	Average number of days between the date of identification of potential suspicious transactions (prior to the analysis of the transaction) and the date when the transaction is reported to the FIU (after the analysis of the transaction) during the last calendar year	x	x	x	x	x	x	x	x	x	x
	Total number of STRs submitted to the FIU during the last calendar year	x	x	x	x	x	x	x	x	x	x
6 - Targeted Financial Sanctions and Compliance with Fund Transfers Regulation	Maximum number of hours between the publication of the TFS by the authorities and the implementation of these changes in the institution's screening tools	x	x	x	x	x	x	x	x	x	x

Category	Data Points	CI	CP	LI	EMI	PI	BC	IF	AMC	CASP	O
	Number of outbound transfers for which requests were received from a counterparty in the transfer chain for information that is missing, incomplete or provided using inadmissible characters in the last calendar year	x	x		x	x				x	x
	Total number of outbound transfers in the last calendar year	x	x		x	x				x	x
	% of outbound transfers rejected or returned by the counterparty in the transfer chain due to information that is missing, incomplete or provided using inadmissible characters in the last calendar year	x	x		x	x				x	x
7 - Group-wide AML/CFT Framework (AML/CFT governance structures, Group-wide ML/TF risk assessment, Group policies and procedures, including sharing of information, Group-wide AML/CFT function)	% of group entities that provided reports to the Group AML compliance on the following areas in the last calendar year (should only be answered by the parent company): a) CDD b) ongoing monitoring c) STRs d) identity and transaction level information on high risk customers e) deficiencies	x	x	x	x	x	x	x	x	x	x
	% of jurisdictions in which the group is established covered by reviews (including access to customer and transaction level data) performed by the group AML/CFT compliance function in the last three calendar years. (applies only to groups that have been existing for more than 3 years and should only be filled in by the parent company)	x	x	x	x	x	x	x	x	x	x
	Number of group entities for which deficiencies were identified by competent AML/CFT supervisors in the last calendar year (should only be filled in by the parent company) - EU/EEA entities - Non-EU/EEA	x	x	x	x	x	x	x	x	x	x

Section C – Datapoints for the calculation of the materiality thresholds for operations under the freedom to provide services

1. List of the European Union countries where the credit or financial institution is operating in practice under freedom to provide services

2. Total number of customers who are resident in the Member State where the credit or financial institution is operating on a freedom to provide service basis, at the end of the last calendar year

2.A. Volumes of transactions generated by the customers under point 2 over the last calendar year

Annex 2 – Interpretive note explaining how the data points listed in Annex 1 should be understood

Section A – Inherent risk data points

Category	Notion / Concept	General explanation
	Sectors	**CI:** credit institutions **CP:** credit providers other than credit institutions **LI:** life insurance undertaking and life insurance intermediaries **EMI:** e-money institutions **PI:** payment institutions **BC:** bureaux de change **IF:** investment firms **AMC:** asset management companies, i.e. companies that manage one or more collective investment undertakings (UCITSs or AIFs) within the meaning of the UCITS and AIFM directives. Where an AMC manages several UCITSs or AIFs, the assessment should be based on aggregated data covering all such UCITSs and AIFs. Where an UCITS or AIF has not designated a management company, the assessment should be based on data covering only the relevant UCITS or AIF. **CASP:** crypto-asset service providers **O:** other financial institutions
-	**Date of reference**	The reference point is always the end of the last calendar year (31 December).
-	**Previous year**	It should refer to the calendar year (from 1.1. until 31.12.) prior to the year of the reporting obligation.
Customers	**Customer**	A natural or legal person who maintains a business relationship with a financial institution in accordance with Article 19(1) AMLR. 'Business relationship' means a business, professional or commercial relationship connected with the professional activities of an obliged entity, which is set up between an obliged entity and a customer, including in the absence of a written contract and which is expected to have, at the time when the contact is established, or which subsequently acquires, an element of repetition or duration. **For LIU and LII:** 'Customer' should refer to the policyholder (natural or legal person) **For AMC:** Customer should refer to the investors of the Collective Investments Undertaking (CIU) for which the Asset Management Company is designated AIFM or UCITS Management Company. If an investor has multiple positions (lines in the shareholder register of the CIU), please count it only once per CIU.
Customers	**LE customer per country**	Per country data should be based on the customers' registration.
Customers	**NP customer per country**	Per country data should be based on the customers' residency. Self-employed persons should be included in this category.
Customers	**PEP**	A PEP means a natural person who is or has been entrusted with prominent public functions following the criteria set by Article 2(34) AMLR, their family members as defined in Article 2(35) AMLR and person known to be a close associate as defined in Article 2(36).
Customers	**PEPs by country**	Please provide the nationality of the Politically Exposed Person (PEP).
Customers	**Customers with at least one transaction**	The transaction must be initiated by the customer, even if it is a periodic/automatic transaction based on a mandate. Only exclude fees that are paid automatically.
Customers	**Non-resident**	Please treat the following categories as non-resident customers 1. legal persons that are domiciled in the country 2. legal arrangements that are administered in the country 3. branches of foreign companies that carry out profit-making activities and are not registered in the business register in the country 4. natural persons who are self-employed as a profession with their headquarters or permanent residence outside of the country 5. natural persons without permanent residence in the country. The obliged entity may decide to obtain this information through the tax number of the customer.

Customers	**Customers with cross-border transactions involving non-EEA countries**	Customers with at least one transaction over EUR 250 from/to a non-EEA country in the previous year. **For LIU and LII:** Gross premiums written/claims received/paid from/to non-EEA countries, if different from the country of residence of the policyholder.
Customers	**Legal entities with complex corporate structure**	A multi-layered structure should be classified in line with Article 12 of the RTS on CDD.
Customers	**Walk-in customer**	Customers who conducted at least one occasional transaction and have not entered into a business relationship with the obliged entity in the previous year.
Customers	**Occasional transaction**	Occasional transaction means a transaction that is not carried out as part of a business relationship as defined in Article 2 (1)(19) of Regulation (EU) 2024/1624.
Customers	**High risk activities**	An 'high-risk activity' should include, at least, the activities mentioned under Annex III of the AMLR.
Customers	**Number of customers with FIU requests linked with AML/CFT**	This information may be collected from the OEs or FIUs and it should refer to the previous year. In case its implementation is complex, you can consider 'number of customers subject to requests from FIU'.
Payment account	**Incoming transactions**	The total value of all incoming payment transactions, as defined by Article 4(5) of Directive 2015/2366/EU (PSD2), credited to payment accounts, as defined by Article 4(12) of PSD2, held by customers with the obliged entity. The following shall be excluded from this calculation: - Internal transfers – The crediting of funds to an account from another account held by the same payment service user within the same obliged entity. - Reversals – Transactions that are subsequently reversed, refunded, or otherwise nullified. In the case of partial reversals, only the unreversed net amount is retained. - Intra-group operational transfers – Transactions credited from an account held by an entity that is part of the obliged entity's consolidation group. This exclusion shall strictly apply only to transactions executed solely for internal operational purposes—such as treasury management, intra-group financing, or internal capital support—and excludes customer-to-customer payments between separate group entities. Furthermore, the exclusion shall not apply to transactions from a group entity where the latter merely intermediates funds originating from a payer outside the group, provided the ultimate payer can be reliably identified from the available payment information. - Incoming e-money payment transactions.
Payment account	**Outgoing transactions**	The total value of all outgoing payment transactions, as defined by Article 4(5) of Directive 2015/2366/EU (PSD2), credited to payment accounts, as defined by Article 4(12) of PSD2, held by customers with the obliged entity. The following shall be excluded from this calculation: - Internal transfers – The crediting of funds to an account from another account held by the same payment service user within the same obliged entity. - Reversals – Transactions that are subsequently reversed, refunded, or otherwise nullified. In the case of partial reversals, only the unreversed net amount is retained. - Intra-group operational transfers – Transactions credited from an account held by an entity that is part of the obliged entity's consolidation group. This exclusion shall strictly apply only to transactions executed solely for internal operational purposes – such as treasury management, intra-group financing, or internal capital support – and excludes customer-to-customer payments between separate group entities. Furthermore, the exclusion shall not apply to transactions from a group entity where the latter merely intermediates funds originating from a payer outside the group, provided the ultimate payer can be reliably identified from the available payment information. - Outgoing e-money payment transactions.
vIBAN	**vIBAN**	Definition used in Article 2(26) AMLR: identifier causing payments to be redirected to a payment account identified by an IBAN different from that identifier. This should include both individual and pooled vIBAN accounts.
vIBAN	**reissued IBAN**	Virtual IBANs where the end user is not a customer of the obliged entity.

Pre-paid cards	**Pre-paid card**	Definition under Article 2(1)(f) of Regulation (EU) 2018/1672: 'Prepaid card' means a non-nominal card that stores or provides access to monetary value or funds which can be used for payment transactions, for acquiring goods or services or for the redemption of currency where such card is not linked to a bank account.
Lending	**Cash collateral**	Collateral which at least partially consists of cash or an account on which cash is deposited as per the definition of cash under Article 2(1)(a) of Regulation (EU) 2018/1672: 'Cash' means: (i) currency; (ii) bearer-negotiable instruments; (iii) commodities used as highly liquid stores of value; (iv) prepaid cards.
Lending	**Outstanding loan**	An outstanding loan refers to the portion of a loan that remains unpaid by the borrower at a given point in time. Credit cards with a credit facility are excluded. Mortgages are excluded.
Lending	**Real estate loans**	Outstanding loans secured by residential real estate collateral, in line with the ECB definition of residential real estate loans.
Lending	**Third party mortgage payments**	Payments and/or interest payments on mortgage loans to be made by third parties/persons not mentioned in the mortgage deed, other than a notary, the national mortgage guarantee (NHG), municipalities or an insurance company.
Lending	**Repaid loans**	The total number of loans that were fully repaid and closed within the reporting year, regardless of their original disbursement date.
Lending	**Prematurely repaid loans**	The total number of loans that were fully repaid and closed within the reporting year, premature to their originally planned disbursement date.
Lending	**Loans that are not associated with the acquisition of any product/service**	Consumer credits and similar credit lines that are granted to customers without specifying a purpose for the credit. The customers are free to decide how they want to use the funds borrowed from the lender.
Life insurance	**Life insurance contracts**	Life insurance products are defined by Article 2(3) of Directive 2009/138/EC.
Life insurance	**Total amount of gross written premiums in the previous year (incoming)**	In accordance with Directive 91/674/EEC, gross premiums written shall comprise all amounts due during the financial year in respect of insurance contracts, arising from gross business, regardless of the fact that such amounts may relate in whole or in part to a later financial year. It includes both direct and reinsurance business. **For LII:** the portion of gross premiums written by the life insurance undertaking in the previous financial year that the relevant life insurance intermediary has distributed.
Life insurance	**Surrender value**	The total amount of surrender value as mentioned in Article 185 (3)(f) of Directive 2009/138/EC, net of taxes. The surrender value should reflect the amount, defined contractually, to be paid to the policyholder in case of early termination of the contract (i.e. before it becomes payable by maturity or occurrence of the insured event, such as death), net of charges and policy loans. It includes surrender values guaranteed and not guaranteed.
Life insurance	**Low risk contracts**	Life insurance contracts or products that meet any of the following conditions: (i) they cannot be redeemed, (ii) contracts merely covering death or certain disabilities or attacks on the physical integrity of the person (which often require medical evidence), which do not include an element of savings or investment, (iii) the annual premium is not above EUR 1 000 or the unique premium is not above EUR 2 500, (iv) contracts whose premiums remain below or equal to applicable tax-deductible ceiling.
Wealth Management	**Customers (NP) that fall under the definition of private banking (RFLGs)**	Private banking encompasses all 'banking and other financial services to high-net worth individuals and their families or businesses', according to the Risk Factor Guidelines (RFLGs). The threshold of EUR 5 000 000 can be used to define high-net worth customers. **For LII and LIU:** This data point is requested for life insurance services provided to high-net-worth customers (NP). - In cases where the policyholder is a legal entity and the insured person is a natural person (for instance, in the case of group contracts), insured persons are to be considered customers even if they are not the policyholder. - For contracts which have two policyholders, both should be considered. The amount should not be divided.
Wealth Management	**assets under management**	**For LIU:** Surrender value for life insurance undertakings. **For LII:** Amount outstanding for life insurance intermediaries.
Investment services	**retail client**	retail clients as defined in MiFID.
Investment services	**professional client**	professional clients as defined in Annex 2 of MIFID.

Investment services	**unlisted financial instruments**	Financial instruments that are not traded on a regulated market, multilateral trading facility (MTF), or organised trading facility (OTF).
Investment services	**AML/CFT regulated customers**	All persons or entities of a similar nature to those listed in Article 3 AMLR, including those that do not fall within the scope of the AMLR due to their non-EU status.
Investment services	**assets under custody**	Refers to the assets for which the investment firm provide safekeeping and administration services (cf. MiFID II – Annex I, Section B – Ancillary services).
Investment services	**asset under management**	Refers to the assets which are either under the scope of a portfolio management mandate or under the scope of an investment advice mandate.
Investment services	**asset held by the customer**	Encompasses assets under custody but also includes assets that the client holds directly or through other intermediaries where the specific firm in question does not have a custody or management role.
Investment services	**Orders transmitted**	Refers to orders forwarded to the market, including unexecuted orders.
Investment services	**final investor**	Refers to the end client or individual who ultimately owns and benefits from the investments, as opposed to intermediaries or entities managing or holding the assets on behalf of others.
Money Remittance	**Money Remittance**	Money Remittance, as defined in Article 4(22) of EU Directive (PSD) 2015/2366, refers to a payment service where funds are received from a payer without the creation of a payment account for the payer or payee, and are then transferred to a payee or another payment service provider acting on the payee's behalf. Essentially, it is a service that facilitates the transfer of money without the need for a bank account at either end.
Correspondent services	**Correspondent services**	Correspondent account established by a respondent institution with a correspondent institution, through which the respondent institution's customers are granted direct access to conduct transactions on the respondent's account.
Correspondent services	**nested account**	Account where a financial institution (the nested financial institution) gains indirect access to services by transacting through another financial institution's (the respondent institution) correspondent account.
Correspondent services	**payable through account**	Correspondent accounts that are used directly by third parties to transact business on their own behalf.
Trade finance	**trade finance**	Financial service or product aimed to be used by customers for the purpose of facilitating international trade and commerce
Trade finance	**trade finance transaction**	A completed trade finance operation that results in an actual transfer of funds. Includes payments under letters of credit, collections, guarantees called upon, or other trade finance instruments that led to cash movement.
Cryptos transactions	**Exchange rate crypto**	The amount/value of crypto transactions is defined according to the legal exchange rate of EUR on the day the transaction is executed.
Cryptos transactions	**Crypto-funds transaction**	Any transaction carried out by the customer whereby the customer exchanges funds against crypto-assets in relation to which the obliged entity provides one or more of the following services in accordance with Article 3(1)(16) of Regulation (EU) 2024/0109: (i) operation of a trading platform for crypto-assets; (ii) exchange of crypto-assets for funds; (iii) exchange of crypto-assets for other crypto-assets; (iv) execution of orders for crypto-assets on behalf of clients; (v) reception and transmission of orders for crypto-assets on behalf of clients; and (vi) providing custody and administration of crypto-assets on behalf of clients.
Cryptos transactions	**Funds-crypto transaction**	Any transaction carried out by the customer whereby the customer exchanges crypto-assets against funds in relation to which the obliged entity provides one or more of the following services in accordance with Article 3(1)(16) of Regulation (EU) 2024/0109: (i) operation of a trading platform for crypto-assets; (ii) exchange of crypto-assets for funds; (iii) exchange of crypto-assets for other crypto-assets; (iv) execution of orders for crypto-assets on behalf of clients; (v) reception and transmission of orders for crypto-assets on behalf of clients; and (vi) providing custody and administration of crypto-assets on behalf of clients.
Cryptos transactions	**Crypto-crypto transaction**	Any transaction carried out by the customer whereby the customer exchanges certain crypto-assets against other crypto-assets in relation to which the obliged entity provides one or more of the following services in accordance with Article 3(1)(16) of Regulation (EU) 2024/0109: (i) operation of a trading platform for crypto-assets; (ii) exchange of crypto-assets for funds; (iii) exchange of crypto-assets for other crypto-assets; (iv) execution of orders for crypto-assets on behalf of clients; (v) reception and transmission of orders for crypto-assets on behalf of clients; and providing custody and administration of crypto-assets on behalf of clients.
Cryptos transactions	**Transfer of crypto-assets**	Any transaction carried out by the customer whereby the customer transfers crypto-assets from one distributed ledger address or account to another, in relation to which the obliged entity provides one or more of the service of transfer referred to in Article 3(1)(16)(j) of Regulation (EU) 2024/0109.
Cryptos transactions	**Unhosted wallets**	Unhosted wallets should refer to the concept of 'self-hosted wallets' as defined in Article 3, point (20), of Regulation (EU) 2023/1113.

Management of UCITS / AIFs	**Retail investor customer**	The person investing in the UCIT or AIF (generally by purchasing the shares issued by such UCIT or AIF), where this person is retail client as defined in MiFID. Where the obliged entity is an asset management company which does not have access to this information (as is often the case in practice), this field is not mandatory.
Management of UCITS / AIFs	**Professional investor customer**	The person investing in the UCIT or AIF (generally by purchasing the shares issued by such UCIT or AIF), where this person is a professional client as defined in MiFID. Where the obliged entity is an asset management company which does not have access to this information (as is often the case in practice), this field is not mandatory.
AIFs	**Open-ended fund**	An open-ended fund is a collective investment vehicle in which investors can subscribe and redeem on-demand.
AIFs	**Close-ended fund**	Collective investment vehicle in which investors cannot subscribe and redeem on-demand.
Safe Custody Services	**Safe deposit boxes**	Safe deposit boxes refer to secure, individually assigned physical storage containers located within a regulated credit institution or financial entity's premises, rented or otherwise made available to customers, typically under a contractual agreement.
Crowdfunding	**Crowdfunding**	Refers to 'crowdfunding services' within the meaning of Article 2(1)(a) of Regulation (EU) 2020/1503.
Crowdfunding	**Donor**	Donor means any natural or legal person who, through a crowdfunding platform, provides funds to a project owner.
Cash transaction	**Cash transaction**	Cash transactions include all movements of physical cash into or out of payment deposit accounts held by natural or legal persons, regardless of the method of deposit or withdrawal. This includes, but is not limited to, over-the-counter cash deposits and withdrawals, ATM transactions, cash-in-transit operations (such as cash courier vans), night safe deposits, bulk cash movements and cash received or deposited by exchanging crypto-assets.
Geographies	**Transaction**	Wire transaction that moves funds from one account to another, either domestically or internationally. This should not include transactions between financial institutions acting on their own behalf, and Internal transfers within the same institution not reflecting customer-originated activity. (This definition applies only to the geographies category). **For LIU and LII:** transfers should include both premiums received and claims paid **For CASP:** In the absence of further information on the country of origin or destination, the determination of such country can be based on the counterparty's IBAN number.
Geographies	**Total value of entity's investment undertakings (CIUs)**	The total value of the investments means the aggregated value of investment flows (asset side) during the previous year (broken down by country the flows come from).
Geographies	**Total value of client assets under management (AMCs)**	The value of assets means the value of assets in the portfolio as of the end of the previous year.
Geographies	**Subsidiaries**	Consider only subsidiaries subject to the AML/CFT laws.
Geographies	**Entity owner/parent company**	This should refer to the ultimate parent company.
Distribution channels	**Remote onboarding**	The customer enters into a relationship with the firm in a non-face-to-face manner.
Distribution channels	**Onboarded by third party**	The customer is introduced by a third party which conducts in full or in parts the CDD arrangements.
Distribution channels	**Distributors**	Refers to Article 3(4) of the Directive 2009/110/EC (E-money Directive).
Distribution channels	**Agents**	**For PI:** An agent within the meaning of Article 4(38) of Directive (EU) 2015/2366 (a natural or legal person who acts on behalf of a payment institution in providing payment services). **For IF:** Agents should be understood as 'tied agents'.
Distribution channels	**White labelling**	Company that collaborates with a licensed obliged entity to offer financial services under its own brand, without having a banking licence itself. While it presented the service to customers, the actual service is legally and operationally provided by the bank. The partner acts as an intermediary between the bank and the customers but not performing any regulated banking activities on its own. Intra-group companies should also be captured.

Section B – AML/CFT Controls data points

Category	Notion / Concept	General explanation
1 - Governance, Culture & Compliance function	**Management body**	The management body as defined in Article 2(1)(37) AMLR, or the compliance manager referred to in Article 11(1) AMLR.
1 - Governance, Culture & Compliance function	**Date at which the procedures covering the entirety of the AML/CFT framework were checked as being in compliance with existing laws and regulations applicable at that date**	If you have more than one date, please use the most recent one. When there is no policy or procedure approved, the answer to the question should be 00-00-00.
1 - Governance, Culture & Compliance function	**Dedicated AML/CFT compliance staff**	Staff mainly focused on AML/CFT compliance-related tasks. This should include at least: - the compliance officer appointed in accordance with Article 11 and all the staff assisting the compliance officer in the tasks defined in Article 11. - staff responsible for carrying out the analysis mentioned in Article 69(2) AMLR and staff responsible for reporting suspicious transactions in accordance with Article 69 AMLR. - staff responsible for establishing and reviewing the internal policies and procedures mentioned in Article 9 AMLR - all other staff specialising in AML/CFT compliance, including those who spend the majority of their time on tasks listed Article 20 AMLR.
1 - Governance, Culture & Compliance function	**AML/CFT training**	Structured education or instruction provided to employees to ensure they understand their legal obligations, institutional policies, and practical procedures for preventing and detecting money laundering and terrorist financing.
1 - Governance, Culture & Compliance function	**Non-AML/CFT specialist staff**	Other relevant staff, with no dedicated AML/CFT functions, who are involved in the performing of AML/CFT duties or perform functions that are relevant from an AML/CFT perspective. This includes, but is not limited to, all staff who are not AML Specialists but who have knowledge of customer and/or transaction information and who should be able to contribute to the detection of facts relevant to Article 69 AMLR (such as front-office staff), internal auditors and senior management.
1 - Governance, Culture & Compliance function	**Agents and distributors**	Agents are intermediaries that are under the full responsibility of a credit or financial institution. Distributors are legal or natural person that can distribute and redeem electronic money pursuant to Article 3(4) of the E-Money Directive (Directive 2009/110/EC).
2 - Internal Controls & Outsourcing	**Compliance Monitoring Check**	Refers to the internal controls and internal audit function that a firm should put in place to monitor and manage compliance with its internal policies and procedures (AMLR, Article 9(2)(a)(vii) and Article 9(2)(b)).
2 - Internal Controls & Outsourcing	**Service providers**	Includes services outsourced within the same group (intragroup outsourcing) must be accounted for.
3 - Risk assessment	**Update of the Customer Risk Assessment (CRA)**	The update refers to the CRA methodology and not to the update of each customer risk score.

3 - Risk assessment	**Number of customers per ML/TF risk category (low risk, medium-low risk, medium-high risk, high-risk)**	In case an entity uses three risk categories Low risk -> Low risk Med risk -> Medium-low risk High risk -> High risk In case an entity uses five risk categories Low risk -> Low risk Medium-low risk -> Low risk Medium-high risk -> Medium-low risk High risk -> Medium-high risk Ultra/very high risk -> High risk
5 - Transaction monitoring and Suspicious Activity Reporting	**Transaction monitoring system**	A system used by the obliged entity to ensure compliance with its obligation to conduct ongoing monitoring of transactions performed by the customer throughout the course of a business relationship in accordance with Article 26 AMLR
5 - Transaction monitoring and Suspicious Activity Reporting	**At least partly automated system**	A system that, as a minimum, automatically generates alerts in order to identify transactions carried out by customers that could potentially be suspicious from an AML/CFT perspective.
5 - Transaction monitoring and Suspicious Activity Reporting	**Non-automated system**	A transaction monitoring system that does not meet the criteria mentioned above.
5 - Transaction monitoring and Suspicious Activity Reporting	**The annual number of transactions exceeds the number of transactions that the obliged entity can manually process**	This option should be selected if the obliged entity does not have the capacity to scrutinise and manually verifyall transactions processed by the obliged entity.
5 - Transaction monitoring and Suspicious Activity Reporting	**Number of days between issuance of the alert and closing of the alert**	Number of calendar days.
5 - Transaction monitoring and Suspicious Activity Reporting	**Ratio between number of alerts and number of STRs**	The data to be provided here is the number of alerts generated by the automated systems and the number of STRs resulting from alerts generated by the automated transaction monitoring systems in accordance with Article 26(1) AMLR. This excludes alerts of systems exclusively meant to detect transaction subject to targeted financial sanctions or politically exposed persons. Numerator: number of STRs Denominator: number of alerts generated by the automated transaction monitoring systems in accordance with Article 26(1) AMLR.
5 - Transaction monitoring and Suspicious Activity Reporting	**The entity has implemented a tool that enables it to analyse the information available on distributed ledgers and generate alerts where unusual patterns or risk factors are identified, in relation to the transactions carried out by the customer**	This datapoint should only be completed by obliged entities providing services under MiCA.
5 - Transaction monitoring and Suspicious Activity Reporting	**Date of identification of potential suspicious transactions**	Date on which a transaction reported as suspicious was first identified as inconsistent with the entity's knowledge of the customer (pursuant to Article 26(1) AMLR), before conducting the assessment of such transactions pursuant to Article 69(2) AMLR.

6 - Targeted Financial Sanctions and Compliance with Fund Transfers Regulation	**Outbound transfers**	The movement of money from a financial account to an external account. This data point only includes transfers at customer level.
6 - Targeted Financial Sanctions and Compliance with Fund Transfers Regulation	**Counter party**	Any legal entity or individual that takes the opposite side of the financial transaction or contract.
7 - Group-wide AML/CFT Framework	**Group-wide AML/CFT function questions**	This question should be answered by the ultimate parent company.
7 - Group-wide AML/CFT Framework	**Group entities**	Entities that are part of the group as defined in Article 2(41) and (42) of Regulation (EU) 2024/1624, including non-EU obliged entities. Entities of the group that are not obliged entities should be excluded from the scope.

European Banking Authority

Tour Europlaza, 20 avenue André Prothin CS 30154
92927 Paris La Défense CEDEX, FRANCE
Tel. +33 1 86 52 70 00
E-mail: info@eba.europa.eu
https://eba.europa.eu