EBA/GL/2023/07

27.11.2023

# Final Report

## Guidelines amending Guidelines EBA/GL/2021/16 on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849 (The Risk-Based Supervision Guidelines)

# Contents

# 1. Executive Summary

These guidelines amend the EBA's revised Risk-Based Supervision Guidelines. They extend the scope of these Guidelines to anti-money laundering and countering the financing of terrorism (AML/CFT) supervisors of crypto-asset service providers as defined in Regulation (EU) 2023/1114 (MiCAR)[1].

Through these amendments, these guidelines foster a common understanding by competent authorities in the EU of the risk-based approach to the AML/CFT supervision of crypto-asset service providers and how it should be applied.

The amendments:

- emphasise the importance of cooperation among competent authorities, prudential supervisors and other stakeholders;
- highlight the importance of a consistent approach to setting supervisory expectations where multiple competent authorities are responsible for the supervision of the same institutions;
- provide guidance on the sources of information available to competent authorities when supervising crypto-asset service providers;
- set out how competent authorities should determine the type of guidance needed within the sector and how to communicate this guidance in the most effective manner; and
- stress the importance of training to ensure that staff from competent authorities are well trained and have the technical skills and expertise necessary for the execution of their functions, including the supervision of crypto-asset service providers.

## Next steps

The guidelines will be translated into the official EU languages and published on the EBA website. The deadline for competent authorities to report whether they comply with the guidelines will be two months after the publication of the translations. The guidelines will apply from 30 December 2024.

[1] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (*OJ L 150, 9.6.2023, p. 40).*

# 2. Background and rationale

## 2.1 Background

1. In July 2021 the European Commission issued a legislative package with four proposals to reform the EU's legal and institutional anti-money laundering and countering the financing of terrorism (AML/CFT) framework. The legislative package included a proposal for a new Regulation (EU) on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.

2. This Regulation (EU) 2023/1113 (recast) (FTR)[2] amends Regulation (EU) 2015/847 and extends its scope to transfers of crypto-assets. It also brings crypto-asset service providers into the scope of Directive (EU) 2015/849 and subjects them to the same AML/CFT requirements and AML/CFT supervision as other credit and financial institutions.

3. The FTR was published in the Official Journal on 9 June 2023 and entered into force on 29 June 2023. It will apply from 30 December 2024. Article 36(3) of this Regulation mandates the EBA to issue guidelines on the risk-based approach to AML/CFT supervision of crypto-asset service providers by competent authorities.

4. In 2023, the EBA performed an analysis of its Risk-Based Supervision Guidelines to establish whether new or additional guidance was necessary to fulfil this mandate.

5. The EBA concluded that the risk-based approach to AML/CFT supervision set out in these Guidelines was adequate and could be extended to AML/CFT supervisors of crypto-asset service providers. It also concluded that several provisions would benefit from further clarification to reflect the nature of crypto-asset services and the impact this has for supervisory purposes.

6. The EBA publicly consulted on a draft version of these amending Guidelines between 29 March 2023 and 29 June 2023. A public hearing took place on 7 June 2023. The Consultation Paper (EBA/CP/2023/05) included several specific questions, which can be found in Section 5.3, for respondents to consider.

7. The EBA received eight responses, including a response from the EBA's Banking Stakeholder Group (BSG). The feedback table in Section 5.4. provides an overview of the consultation responses received by the EBA and of the EBA's assessment of these responses, and explains the changes that the EBA decided to make to the draft amending Guidelines as a result.

8. These guidelines amend the revised Risk-Based Supervision Guidelines. A consolidated version will be published on the EBA's website.

[2] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (recast); (OJ L 150/ 9.6.2023, p.1).

## 2.2 Rationale

9. This section explains the rationale for the amendments to the revised Risk-Based Supervision Guidelines.

### Amendments to 'Subject matter, scope and definitions'

10. Article 36(3) FTR mandates the EBA to issue guidelines on the risk-based approach to the AML/CFT supervision of crypto-asset service providers by competent authorities. This is why the EBA included this mandate in the subject matter of the existing guidelines.

11. The amending Guidelines provide further clarification that the definitions as set out in Directive (EU) 2015/849 and Regulation (EU) 2023/1113[3] also apply in these guidelines.

### Amendments to 'Guideline 4.1: Implementing the RBS Model'

12. This guideline contains a reference to the EBA Guidelines on internal governance[4] that do not apply to AML/CFT supervisors of crypto-asset service providers. The provisions in these guidelines are nevertheless relevant and AML/CFT supervisors should consider applying these guidelines since relevant guidelines under Regulation (EU) 2023/1114[5] are not foreseen.

### Amendments to 'Guideline 4.2: Step 1 – Identification of risk and mitigating factors'

13. The guidelines provide that competent authorities should identify and understand the risk factors that will affect each sector and subject of assessment's exposure to ML/TF risks. Competent authorities should identify these risk factors based on information from a variety of sources. The amendments to this guideline provide guidance on the sources of information available to competent authorities when supervising crypto-asset service providers.

14. The EBA also included a direct reference to crypto-asset service providers to ensure that they are now considered in scope where relevant to their supervisory work.

### Amendments to 'Guideline 4.3: Step 2 – Risk assessment'

15. Competent authorities should assess the extent to which AML/CFT systems and controls are adequate to effectively mitigate the inherent risks to which the subject of assessment is exposed. The EBA included a reference to Article 19a of Directive (EU) 2015/849 to provide for the specific AML/CFT systems and controls that crypto-asset service providers should have put in place and should apply.

### Amendments to 'Guideline 4.4: Step 3 – Supervision'

16. Competent authorities should determine and implement a longer-term AML/CFT supervisory strategy. In the strategy, competent authorities should set clear objectives for their approach to AML/CFT supervision and set out how these objectives will be achieved within a defined timeframe

[3] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (recast); (OJ L 150/ 9.6.2023, p.1).

[4] EBA's Guidelines on internal governance under Directive (EU) 2019/2034, EBA/GL/2021/14.

[5] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (*OJ L 150, 9.6.2023, p. 40).* The issuance of these guidelines will be aligned both with the entry into force of the recast FTR and new MiCAR.

and with available resources. As part of this, they should determine the supervisory resources necessary to implement the supervisory strategy and ensure that sufficient resources are available to them. When determining the necessary resources, competent authorities should also consider the technological resources they need to perform their functions effectively, for example to be able to assess the adequacy of any software or other technological tools their subjects of assessment use to comply with their AML/CFT obligations. This will be particularly important where technology is essential to how the specific sectors operate.

17. In addition, the EBA's amendments set out how competent authorities should determine the type of guidance needed within the sector and how to communicate this guidance in the most effective manner.

18. Finally, the amendments stress the importance of training to ensure that staff from competent authorities are well trained and have the tools, technical skills, and expertise necessary for the execution of their functions, including the supervision of crypto-asset service providers, and that they use these tools as appropriate in a risk-based approach.

### Amendments to 'Guideline 4.5: Step 4 – Monitoring and updating of the RBS Model'

19. Competent authorities should periodically review whether their AML/CFT RBS Model delivers the intended outcome. Competent authorities should use a variety of tools available to them when reviewing and assessing the adequacy and effectiveness of their AML/CFT RBS Model. In its amendments, the EBA emphasises the importance of technical expertise when reviewing and assessing the adequacy and effectiveness of competent authorities' AML/CFT RBS Model, considering the fast-paced technological developments.

### Editorial amendments to reflect the scope of the supervisory work

20. Finally, the EBA made a number of changes that are of an editorial, a presentational or a structural nature such as updating footnotes.

# 3. Guidelines amending the Risk-Based Supervision Guidelines

EBA/GL/2023/07

27 November 2023

# Guidelines amending Guidelines EBA/GL/2021/16

## on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849

## The Risk-Based Supervision Guidelines

# 1. Compliance and reporting obligations

## Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[6]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

2. Guidelines set the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

## Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by [dd.mm.yyyy]. In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website with the reference 'EBA/GL/2023/07'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[6] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

# 2. Subject matter, scope and definitions

## Addressees

5. These guidelines are addressed to competent authorities as defined in Article 4 point (2)(iii) of Regulation (EU) No 1093/2010.

# 3. Implementation

## Date of application

6. These guidelines apply from 30 December 2024.

# 4. Amendments

### i. Amendments to 'Subject matter, scope and definitions'

7. Paragraph 5 is amended as follows:

'These guidelines specify in accordance with Article 48(10) of Directive (EU) 2015/849[7] and Article 36(3) of Regulation (EU) 2023/1113[8] the characteristics of a risk-based approach to anti-money laundering and countering the financing of terrorism (AML/CFT) supervision and the steps competent authorities should take when conducting AML/CFT supervision on a risk-sensitive basis.'

8. Paragraph 8 is amended as follows:

'Unless otherwise specified, the terms used and defined in Directive (EU) 2015/849 and Regulation (EU) 2023/1113 have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply.'

### ii. Amendments to 'Guideline 4.1: Implementing the RBS Model'

#### 4.1.3 Subjects of assessment

9. Paragraph 19 is amended as follows:

'Where a competent authority knows, or has reasonable grounds to suspect, that the risk associated with an individual credit institution or financial institution in a cluster varies significantly from that associated with other credit institutions or financial institutions in that cluster, the competent authority should remove that credit institution or financial institution from the cluster and assess it either individually, or as part of a different cluster of credit institutions or financial institutions, which are exposed to a similar level of ML/TF risk. The removal from a cluster should include, inter alia, circumstances where:

- the credit institution or financial institution is beneficially owned by individuals whose integrity is in doubt due to ML/TF concerns; or
- the credit institution's or financial institution's internal control framework is deficient which has an impact on the credit institution's, or financial institution's residual risk rating; or
- the credit institution or financial institution has introduced significant changes to its

[7] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73–117).

[8] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (recast) (OJ L 150/ 9.6.2023, p.1).

products or services, or may have combined those changes with changes in delivery channels, its customer base or different geographic areas where the services or products are delivered.

When assessing these points, competent authorities should take into account suitability assessments made under the prudential frameworks, in particular, where applicable, assessments in relation to the suitability of members of the management body and of the heads of internal control functions, including those assessments made under the joint ESMA and EBA 'fit and proper' guidelines[9] and the EBA Guidelines on internal governance[10].

In the case of crypto-asset service providers, competent authorities should consider applying Sections 1, 2, 3 and 5 of Title II, Section 6 of Title III, Sections 8 and 9 of Title IV and Title V of the EBA Guidelines on internal governance for investment firms[11] for AML/CFT purposes.[12]'

#### 4.1.4 Cooperation

10. Paragraph 22 is amended as follows:

'Competent authorities should consider the objective of their cooperation and information exchange with other stakeholders, and on this basis determine the most effective way for this cooperation, as the same approach may not be suitable in all circumstances. Competent authorities should in particular ensure that they cooperate effectively with those authorities that are responsible for the conduct and prudential supervision of the same subject of assessment.'

### iii. Amendments to 'Guideline 4.2: Step 1 – Identification of risk and mitigating factors'

#### 4.2.2 Sources of information

11. In paragraph 31 the following new points are inserted:

'k) outcomes of analysis of one or more advanced analytics tools; or'

'l) notifications of repeatedly failing payment service providers or crypto-asset service providers submitted to the responsible competent authorities in accordance with Articles 8(2), 12(2), 17(2) and 21(2) of Regulation (EU) 2023/1113, to the extent that these providers fall within the competent authority's supervisory scope.'

[9] Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU, EBA/GL/2021/06.

[10] The EBA's Guidelines on internal governance under Directive 2013/36/EU, EBA/GL/2021/05.

[11] The EBA's Guidelines on internal governance under Directive (EU) 2019/2034, EBA/GL/2021/14.

[12] This is without prejudice to Article 68 of Regulation (EU) 2023/1114 (MiCA) regarding governance arrangements for crypto-asset service providers.

### 4.2.5 Sector-wide ML/TF risk factors

12. Paragraph 37 is amended as follows:

'Competent authorities should have a good understanding of the risk factors that are relevant for all sectors under their supervision. In order to identify relevant risk factors in the relevant sectors, competent authorities should first define the sectors under their supervision. To inform their view of the sectors, competent authorities should categorise obliged entities in line with the list of institutions provided in the definition of credit and financial institutions under Article 3(1) and (2) of Directive (EU) 2015/849.'

13. Paragraph 38 is amended as follows:

'Depending on the size of a sector and the nature of subjects of assessment within it, competent authorities should consider dividing sectors further into subsectors. This may be necessary when a sector is made up of subjects of assessment that are very diverse because a substantial proportion of subjects of assessment share similar features and business models that set them apart from the rest of the sector. Similar features include, but are not limited to, the type of products and services offered, the delivery channels used and the type of customers they service. Examples of subsectors include money-remitters, private banks, brokerage firms, and crypto-asset exchanges, which represent subsectors of payment institutions, credit institutions, investment firms, and crypto-asset service providers respectively. To inform their view on sectors and subsectors and their specific features, competent authorities should refer to Title II of the EBA's AML/CFT Risk Factors Guidelines.'

### 4.2.6 Type of information necessary to identify risk factors

14. In paragraph 41 point l) is inserted:

'l) where the use of technology, such as distributed ledger technology (DLT) or anonymity enhancing features, is essential to the sector's or subsector's business model and operation, the effect this technology has on the sector's or subsector's ML/TF risk exposure.'

15. Paragraph 44 point c) and point f) are amended as follows:

'c) the nature and complexity of the products and services provided and the type of transactions carried out;'

'f) the geographical area of the business activities, in particular where they involve high-risk third countries[13], including, where applicable, the countries of origin or establishment of a

[13] EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849, EBA/GL/2021/02.

significant part of the subject of assessment's customers and the geographical links of its qualifying shareholders or beneficial owners;'

16. In paragraph 45 point a) the following indent is inserted:

'v) from advanced analytics tools and platforms where services of the subject of assessment are provided using DLT or blockchain technology.'

### iv. Amendments to 'Guideline 4.3: Step 2 – Risk assessment'

#### 4.3.3 Individual risk assessments

17. Paragraph 59 point a) is amended as follows:

'a) that the AML/CFT systems and controls listed in Articles 8(4) and 19a of Directive (EU) 2015/849 are put in place and applied. These controls should be sufficiently comprehensive and commensurate with the ML/TF risks;'

### v. Amendments to 'Guideline 4.4: Step 3 – Supervision'

#### 4.4.2 Supervisory strategy

18. Paragraph 78 point e) is amended as follows:

'e) determine the supervisory resources necessary to implement the supervisory strategy and ensure that sufficient resources are available to them. When determining the necessary resources, competent authorities should also consider the technological resources they need to perform their functions effectively, in particular where technology is essential to how the specific sectors operate;'

#### 4.4.4 Supervisory tools

19. Paragraph 94 is amended as follows:

'In some instances, competent authorities should consider whether the combination of two or more tools may be more effective. This includes situations where the competent authority is concerned about the accuracy of information received during off-site reviews or as part of AML/CFT returns. In such circumstances, it may be necessary for competent authorities to verify this information through an on-site inspection, which generally contains such elements as sampling of transactions and customer files, and interviews with key personnel and members of the management body. Competent authorities should be able to carry out ad hoc inspections when necessary, which do not form part of their supervisory strategy and plan. The need for such inspections may be triggered by a specific event, which may expose the sector/subsector or subjects of assessment to an increased ML/TF risk, or by significant

changes in the ML/TF risk exposure of the sector/subsector or subjects of assessment, or may happen as a result of discovery of certain information by the competent authority, including through whistleblowing reports, widespread public allegations of wrongdoing, information from other public domestic or foreign authorities, a new ML/TF typology or supervisory findings relating to AML/CFT systems and controls or a wider internal controls framework. Where the competent authority has decided that an ad hoc inspection is warranted, it should determine the scope of the inspection, the focus of the inspection and whether it will involve any on-site elements, and if there is a need to involve and cooperate with other supervisors.'

### 4.4.5 Supervisory practices and the supervisory manual

20. Paragraph 101 point c) indent i) is amended as follows:

'i) the adequacy of relevant policies and procedures and whether they are linked to the business-wide risk assessment and whether these policies and procedures are reviewed and, if necessary, updated whenever the business-wide risk assessment changes;'

### 4.4.8 Supervisory follow-up

21. Paragraph 117 is amended as follows:

'Where competent authorities have suspicions that the failure to implement effective systems and controls may be deliberate, they should consider a more robust follow-up action, which would ensure an immediate cessation of such behaviour by the subject of assessment. In such circumstances, competent authorities should cooperate with and exchange information on and, where necessary, coordinate actions with respect to the subject of assessment's failures with prudential supervisors.'

### 4.4.9 Feedback to the sector

22. In paragraph 125 point f) is inserted:

'f) concerns about the quality and usefulness of suspicious transaction reports.'

23. Paragraph 126 point a) and point b) are amended as follows:

'a) facilitates and supports the implementation, by subjects of assessment, of an effective risk-based approach, including through the publication of best practices identified in the sector;'

'b) does not directly or indirectly foster or condone unwarranted de-risking of entire categories of customers in accordance with the Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when

providing access to financial services under Directive (EU) 2015/849 and the EBA's ML/TF Risk Factor Guidelines and in particular guidelines 4.9., 4.10. and 4.11.[14];'

24. In paragraph 126 point c) is inserted:

'c) where multiple competent authorities are responsible for the AML/CFT supervision of subjects of assessment in the same sector in the Member State, these competent authorities should coordinate their actions and consider issuing joint guidance to set consistent expectations. Competent authorities should consider whether other authorities may be responsible for issuing guidance on related matters and, if so, coordinate with those authorities as appropriate.'

25. Paragraph 127 is amended as follows:

'Competent authorities should consider engaging with subjects of assessment and other relevant stakeholders when developing supervisory guidance and should determine the most effective way for this outreach. The engagement may include, among other things, a public consultation process, engagement with the sector, in particular where a sector is new to regulation or supervision, engagement with trade associations, financial intelligence units, law enforcement, other competent authorities or government agencies, or participation in consultative forums. Competent authorities should ensure that the outreach includes a sufficient proportion of stakeholders who will be impacted by the guidance and that sufficient time is allocated for stakeholders to communicate their views.'

26. Paragraph 128 is amended as follows:

'Competent authorities should periodically assess the adequacy of their existing guidance provided to the sector, in particular where a sector is new to regulation or supervision. Such an assessment should be done regularly or on an ad hoc basis, and may be triggered by certain events, including changes in the national or European legislation or amendments to the national or supranational risk assessment, or may be based on the feedback from the sector. Where competent authorities determine that the existing guidance is no longer up to date or relevant, they should communicate the necessary amendments to the sector without undue delay.'

[14] EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849, EBA/GL/2021/02.

### 4.4.10 Training of competent authority's staff

27. Paragraph 133 is amended as follows:

'Competent authorities should develop a training programme, which should be adjusted to meet the needs of specific functions within the competent authority, taking into account the characteristics of the sectors under their supervision, their job responsibilities, seniority and experience of staff. Competent authorities should keep this training programme up to date and review it regularly to ensure that it remains relevant.

Competent authorities should ensure that the training provided is sufficiently comprehensive so that relevant staff have adequate technical expertise for the supervision of the subjects of assessment. If necessary, competent authorities should engage an external training provider.

Competent authorities should monitor the level of training completed by individual staff members or entire teams as appropriate.'

28. A new paragraph 133A is inserted:

'133A. Where competent authorities use services of external parties to carry out (some parts of) their supervisory plan or a specific supervisory task as referred to in Section 4.4.7, or otherwise delegate supervisory tasks to other supervisory authorities, competent authorities should also consider including any such external party within their training programme.'

29. Paragraph 134 point c) and point d) are amended as follows:

'c) assess the adequacy, proportionality and effectiveness of subjects of assessment's AML/CFT policies and procedures, including any software or other technological tools, and wider governance arrangements and internal controls in light of subjects of assessment's own risk assessment and business models;'

'd) understand different products, services and financial instruments, and the risks to which they are exposed, including those associated with the underlying technologies used in the provision of those products, services and instruments;'

30. In paragraph 134 point g) is inserted:

'g) understand the technology underpinning the business models, operations and controls of subjects of assessment to be able to assess the risks and controls and to enable the appropriate deployment of (technology-enabled) supervisory tools.'

31. Paragraph 135 is amended as follows:

'Training should be tailored to the AML/CFT responsibilities of relevant staff, and senior management, and may include internal and external training courses and conferences, e-learning courses, newsletters, case study discussions, recruitment, feedback on completed tasks, and other forms of 'learning by doing'. Where necessary and appropriate, competent authorities should also consider filling existing knowledge gaps through strategic hires or draw on the support of in-house specialists such as IT specialists.'

32. A new paragraph 135A is inserted:

'135A. Where multiple competent authorities are responsible for the AML/CFT supervision of the same sector in the Member State, competent authorities should consider providing joint training, to achieve a common understanding of the applicable framework and how it should be applied, and a consistent supervisory approach. Competent authorities may also benefit from knowledge sharing among competent authorities and with other relevant domestic and foreign authorities, such as prudential supervisors, the FIU, relevant EU bodies, and other countries' AML/CFT supervisors.'

### vi. Amendments to 'Guideline 4.5: Step 4 – Monitoring and updating of the RBS Model'

#### 4.5.2 Review of the AML/CFT RBS Model

33. In paragraph 148 point a) is amended as follows:

'a) Professional and technical expertise;'

# 5. Accompanying documents

## 5.1 Cost-benefit analysis / impact assessment

As per Article 16(2) of Regulation (EU) No 1093/2010 (EBA Regulation), any guidelines and recommendations developed by the EBA shall be accompanied by an impact assessment (IA), which analyses 'the potential related costs and benefits'. This analysis presents the IA of the main policy options included in this Final Report on *Guidelines amending the revised Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing ('ML/TF') supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849 (amending the Joint Guidelines ESAs 2016 72)* ('the amending Guidelines'). The IA is high-level and qualitative in nature.

### A. Problem identification and background

Directive (EU) 2015/849, in line with international standards in combating money laundering and the financing of terrorism developed by the FATF, puts the risk-based approach at the centre of the EU's ML/TF regime, and Article 48(6) thereof requires competent authorities, when carrying out risk-based supervision, to have a clear understanding of ML/TF risks in their jurisdiction, to have access to relevant information through both on-site and off-site supervisory activities, and to adjust the intensity and frequency of their risk-based supervision in line with the level of ML/TF risk presented by firms under their supervision. These requirements were complemented by the mandate given to the EBA under Article 48(10) of the same Directive requesting it to issue guidelines containing the characteristics of a risk-based approach and the steps to be taken to conduct risk-based supervision. In this context, the EBA, together with EIOPA and ESMA, published the Joint Guidelines ESAs/2016/72 on 16 November 2016. In order to be in line with the updated ML/TF framework, these Guidelines were revised in December 2021 when the EBA published *the revised Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849 (amending the Joint Guidelines ESAs 2016 72)* ('the revised Guidelines').

Besides, in July 2021, the European Commission published an AML/CFT package consisting of four legislative proposals. One of these proposals was the recast of Regulation (EU) 2015/847 ('the Funds Transfer Regulation' or 'FTR') in order to extend its scope to transfers of crypto-assets, in line with the FATF's standards. The co-legislators reached a provisional agreement on the FTR recast on 29 June 2022. In this provisional agreement the EBA was given ten legislative mandates and one of them was given by its Article 30: *'The EBA shall issue guidelines, addressed to competent authorities, on the characteristics of a risk-based approach to supervision of crypto-asset service providers and the steps to be taken when conducting supervision on a risk-based basis'*. Then, on 9 June 2023, the FTR recast was officially published as Regulation (EU) 2023/1113 ('the FTR recast') and entered into

force on 29 June 2023. Article 36 of the FTR recast confirmed the mandate of the provisional agreement: *'EBA shall issue guidelines, addressed to competent authorities, on the characteristics of a risk-based approach to supervision of crypto-asset service providers and the steps to be taken when conducting such supervision'.* Hence Article 38 of the recast FTR amends Article 3(2) of Directive (EU) 2015/849 to subject crypto-asset service providers ('CASPs') to the same ML/TF requirements and ML/TF supervision as credit and financial institutions.

To meet this mandate of Article 36 of the FTR recast, the EBA's view is to leverage on the revised Guidelines.

### B. Policy objectives

Following the above-mentioned changes, the objectives are to ensure that the revised Guidelines will guide competent authorities on the characteristics of a risk-based approach to supervision of CASPs and the steps to be taken when conducting their supervision on a risk-based basis.

### C. Options considered, assessment of the options and preferred options

Section C presents the main policy options discussed and the decisions made by the EBA during the development of the amending Guidelines. Advantages and disadvantages, as well as potential costs and benefits from the qualitative perspective of the policy options and the preferred options resulting from this analysis, are provided.

#### Inclusion of CASPs in the revised Guidelines

The revised Guidelines are addressed to the competent authorities (CAs) in their supervision of credit and financial institutions but were not covering supervision of all CASPs as CASPs did not fall under the definition of credit or financial institutions (only two types of CASPs – providers engaged in exchange services between virtual currencies and fiat currencies, and custodian wallet providers – were obliged entities). With the FTR recast and the modification of Article 3(2) of Directive (EU) 2015/849, all CASPs will be included in the definition of 'financial institutions' and, de facto, included in the revised Guidelines. In this context, two options have been considered by the EBA in this regard:

**Option 1a: Not amending the revised Guidelines further than the de facto inclusion of the CASPs in the definition of 'financial institutions' foreseen by the modification of Article 3(2) of Directive (EU) 2015/849**

**Option 1b: Amending the revised Guidelines further than the de facto inclusion of the CASPs in the definition of 'financial institutions' foreseen by the modification of Article 3(2) of Directive (EU) 2015/849 in order to reflect CASPs' supervision specificities**

The EBA performed a review of the revised Guidelines and noticed that the risk-based approach to ML/TF supervision set out in these guidelines could be extended to AML/CFT supervisors of CASPs

but also that several provisions would benefit from further clarification to reflect the nature of crypto-asset services and the impact this has for supervisory purposes. For instance, CASPs particularities that would benefit from additional guidance are their technical characteristics like specific infrastructure technology (such as distributed ledger technology (DLT)). Indeed, the competent authorities would, for instance, have to adapt to this new technology in connection with the type of information necessary to identify risk factors, with the risk assessment, and with the human resources (i.e. competent authorities' staff trainings) dedicated to such supervision. The costs related to the amendments of the revised Guidelines would not be material as the main costs are not triggered by these amendments but by the FTR recast and the modification of Article 3(2) of Directive (EU) 2015/849, where the CASPs were included in the 'financial institutions' definition and, de facto, included in the revised Guidelines. As such, the costs of the amending Guidelines would be exceeded by the previously mentioned benefits.

On these grounds, **Option 1b has been chosen as the preferred option** and the amending Guidelines will amend the revised Guidelines further than the inclusion of the CASPs in the definition of 'financial institutions' foreseen by the modification of Article 3(2) of Directive (EU) 2015/849.

### D. Conclusion

The development of Guidelines amending the revised Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing ('ML/TF') supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849 (amending the Joint Guidelines ESAs 2016 72) was deemed necessary to reflect the nature of CASPs and the impact this has for supervisory purposes. The costs associated with the amendments of the revised Guidelines will be exceeded by the aforementioned benefits. The amending Guidelines hence should achieve, with acceptable costs, their objectives of ensuring that the Risk-Based Supervision Guidelines will guide competent authorities on the characteristics of a risk-based approach to supervision of CASPs and the steps to be taken when conducting their supervision on a risk-based basis.

## 5.2 Views of the Banking Stakeholder Group (BSG)

### General comments

The BSG state that they welcome the early consultation by the EBA to prepare for the inclusion of AML/CFT supervisors of crypto-asset service providers within the scope of the EBA's Risk-Based Supervision Guidelines. The BSG also welcome the EBA's recognition that some further clarification is likely to be helpful to ensure that the guidelines can be effectively applied.

The BSG recognise that many of the EBA's proposed amendments are technical in nature, serving mainly to reference the new legislation, mandate, and scope. The BSG have not commented on these.

The BSG state that they welcome the inclusion of references to the need for supervisors to consider and understand technologies that are key to the delivery of crypto-asset services and which may be useful in AML controls. The BSG consider such understanding important to ensure that risks are understood, that the quality of firms' controls can be appropriately understood, and that efficient and effective use is made of opportunities to deploy technology in AML controls and supervision which may be different from those used for 'traditional' transaction monitoring.

The BSG think it would be helpful to go further and include references to the need to understand and consider how choices about technology can affect the AML risk profile of crypto-asset services, e.g. there may be differences arising from whether CASPs are centralised or decentralised in nature, whether crypto-asset wallets are open-source or proprietary, whether the ledger is permissioned or permissionless, the degree of anonymity permitted, and the extent to which anonymity is actively facilitated, for example through the use of mixers or embedded anonymisation technologies within the crypto-asset itself. The BSG suggested ways to include this.

The BSG state that they also welcome the emphasis on the importance of coordination between competent authorities and consistency of approach, stating that this is beneficial both for the achievement of the authorities' objectives and for regulated entities.

In their response to Question 1: Do you have any comments with the proposed changes to the 'Subject matter, scope and definitions', the BSG indicate that they support the European Parliament's and Council's readiness to make CASPs eligible for direct AMLA supervision, and they encourage the decision-makers in the trilogue negotiations to extend the list of obliged entities accordingly.

The BSG note that if CASPs are at the same time financial institutions, they will in any case be AML-supervised by the financial supervisory authorities in their respective Member State at least, possibly also by the AMLA if they are significant and meet the criteria for AMLA supervision. Against this backdrop, the BSG find it particularly important to also include CASPs that are not financial institutions under AMLA supervision, in order to ensure a level playing field in the EU single market for financial services.

In their response to Question 2: Do you have any comments with the proposed changes to the Guideline 4.1 'Implementing the RBS model', the BSG indicate that they are content with the proposed amendments.

In their response to Question 3: Do you have any comments on the proposed changes to the Guideline 4.2 'Step 1 – Identification of risk and mitigating factors', the BSG welcome the amendment to paragraph 41 but find it as currently drafted to be too high-level to provide assurance that the implications of the technology for ML/TF risks will be identified and understood. The BSG think it is important to indicate that there are choices about how technology is used which impact the business model and the ML/TF risk. The BSG state that one approach would be to incorporate specific examples – such as the choice between permissioned and permissionless ledgers or the use of mixers to disguise the origin of coins in a transaction. However, the BSG propose a drafting in more general terms to allow for evolution of the technology. The BSG therefore suggest adding to paragraph 41 a new point l) as follows:
'l) the (infrastructure) technology prevalent in the sector, in particular where this is essential to the sector's business model and operation (such as Distributed Ledger Technology (DLT)) **and where choices about how such technology is deployed affect the susceptibility of the business to use for ML/TF purposes (such as technology which facilitates anonymity or masks the origin of funds)**.'

Regarding the amendment to paragraph 45 under a) subparagraph v), the BSG state they welcome the recognition that there are different tools available for the monitoring/analysis of transactions using DLT and that this is a factor competent authorities need to consider.

The BSG are content with the other proposed amendments.

In their response to Question 4: Do you have any comments on the proposed changes to the Guideline 4.3 'Step 2 – Risk assessment', the BSG indicate that they are content with the proposed amendments.

In their response to Question 5: Do you have any comments with the proposed changes to the Guideline 4.4 'Step 3 – Supervision', the BSG state that they welcome the recognition in paragraph 78 subparagraph e) that competent authorities will need to consider what technology they themselves need, stating that it will be essential to ensure that their supervision is both effective and efficient given the specific tools available where (for example) DLTs are used.

The BSG propose one small addition to reflect the fact that competent authority staff need to understand the relevant technology and how to use the tools too. The BSG state that competent authorities need to avoid behaviour that they would criticise in a supervised firm, such as buying an off-the-shelf IT tool without configuring and using it appropriately or being able to sensibly interpret what it is telling them:

'e) determine the supervisory resources necessary to implement the supervisory strategy and ensure that sufficient resources are available to them. When determining the necessary resources, competent authorities should also consider the technological resources they need to perform their functions effectively, in particular where technology is essential to how the specific sectors operate**,**

**and the need for staff to have sufficient understanding of technologies and tools to deploy them appropriately**;'

The BSG consider that it is appropriate to include this addition here and not only in paragraphs 132–136 which deal with staff training, as they argue that those paragraphs focus more on equipping staff to understand and use the supervisory strategy and tools, rather than the expertise needed to design the framework and tools in practice, which they consider to also be relevant here.

Regarding the amendments to paragraphs 133, 133A, 134 letter c, 134 letter d, 135 and 135A**,** the BSG state they welcome the addition of a reference to the need for appropriate 'technical expertise' in paragraph 133. In their view, taken together with the revised version of this section, this could be understood as including a sufficient understanding of technology where key to business models, the assessment of risks, and deployment of supervisory tools, but the BSG feel there is scope for ambiguity. The BSG think it would be preferable to include an explicit reference given the unavoidable need for such expertise in relation to the supervision of CASPs in particular.

According to the BSG the explicit reference could be included in various parts of this section. The BSG suggest adding it into paragraph 133 as follows:

133. Competent authorities should develop a training programme, which should be adjusted to meet the needs of specific functions within the competent authority, taking into account the characteristics of the sectors under their supervision, their job responsibilities, seniority and experience of staff. Competent authorities should ensure that relevant staff has sufficient technical expertise for the supervision of the subjects of assessment**, including appropriate technological expertise where intrinsic to the business model, operations or controls of the entities supervised**. This training program should be kept up to date and reviewed regularly. Competent authorities should monitor the level of training completed by individual staff members or entire teams as appropriate.

The BSG also propose adding a new point g) at the end of paragraph 134 as follows:

**g) understand the technology underpinning business models, operations or controls of supervised entities or supervisory tools sufficiently to assess the risks and controls of supervised entities and to enable the appropriate deployment of technology-enabled supervisory tools.**

The BSG are content with the other proposed amendments.

In their response to Question 6: Do you have any comments on the proposed changes to the Guideline 4.5 'Step 4 – Monitoring and updating of the RBS model', the BSG indicate that they are content with the proposed amendments.

## 5.3 Feedback on the public consultation and on the opinion of the BSG

The EBA publicly consulted on the draft guidelines contained in the consultation paper amending the revised Risk-Based Supervision Guidelines. The consultation period lasted for three months and ended on 29 June 2023. Eight responses were received, of which five 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 detail on other comments received, the analysis performed by the EBA triggered by these comments, and the actions taken to address them if deemed necessary.

In those instances where several respondents made similar comments or the same respondent repeated its comments in the response to different questions, the comments and the EBA analysis are included where the EBA considers them most appropriate. Changes to the draft guidelines have been incorporated as a result of the responses received during the public consultation.

### Summary of key issues and the EBA's response

The EBA asked respondents to reply to the following six questions:

1. Do you have any comments with the proposed changes to the 'Subject matter, scope and definitions'?

2. Do you have any comments with the proposed changes to the Guideline 4.1 'Implementing the RBS model'?

3. Do you have any comments on the proposed changes to the Guideline 4.2 'Step 1 – Identification of risk and mitigating factors'?

4. Do you have any comments on the proposed changes to the Guideline 4.3 'Step 2 – Risk assessment'?

5. Do you have any comments with the proposed changes to the Guideline 4.4 'Step 3 – Supervision'?

6. Do you have any comments on the proposed changes to the Guideline 4.5 'Step 4 – Monitoring and updating of the RBS model'?

Respondents broadly welcomed the changes proposed by the EBA. They found that the amendments were conducive to a common understanding of the components necessary for an effective AML/CFT supervision of CASPs and ensuring a level playing field for financial and credit institutions, including CASPs. Where respondents made comments, these related to timing and legal uncertainty, the specificities of CASPs that may warrant a unique approach, and competent authorities' ability to supervise CASPs.

### Timing

Some respondents were concerned about the timing of the consultation and the legal uncertainty they felt this created for competent authorities and CASPs. They stated that parts of the consultation contained references to draft legislation that was subject to change. Respondents asked the EBA to wait until the legislation was finalised.

The consultation paper reflects the political compromise available at the time. When finalising the guidelines, the EBA adjusted the consultation paper where necessary to reflect the wording of Regulation (EU) 2023/1113 (FTR) that had since been adopted. The EBA did not identify any differences that have a material effect on these guidelines. At the same time, CASPs are associated with a higher level of ML/TF risk as mentioned in the EBA's fourth Opinion on ML/TF risks[15]. That is why the EBA is setting common standards at an early stage to support competent authorities as they develop and put in place their approaches to AML/CFT supervision of CASPs, thereby preventing these risks from amplifying.

### Specificities of CASPs

Another theme concerned the specificities of CASPs that some respondents argued warranted specific treatment e.g. specific guidelines to be issued under Regulation (EU) 2023/1114 (MiCA)[16].

The EBA recognises the specificities of CASPs and reflected these in these guidelines. Following the consultation, the EBA amended several provisions in these guidelines to further clarify the nature of crypto-asset services and the impact this has for supervisory purposes where necessary. The EBA remains of the view that, in line with international standards and good practice, the risk-based approach to AML/CFT supervision set out in these guidelines should be extended to AML/CFT supervisors of CASPs.

### Competent authorities

Some respondents were concerned that competent authorities would not be equipped to adequately supervise CASPs e.g. due to a lack of understanding of the ML/TF implications the technology used by subjects of assessment has or because of inexperience with the use of technology by competent authorities for supervisory purposes.

The EBA agrees that supervisors need to have the necessary skills to perform their respective functions effectively. That is why the EBA in the amending Guidelines further stresses the importance of training to ensure that supervisors understand the technology underpinning the business models, operations and control framework of subjects of assessment and that they use adequate tools to supervise institutions within their remit, including CASPs.

[15] EBA publishes fourth Opinion on money laundering and terrorist financing risks across the EU | European Banking Authority (europa.eu).

[16] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 9.6.2023, p. 40).

## 5.4 Summary of responses to the consultation and the EBA's analysis

| Guideline | Summary of responses received | EBA analysis | Amendments to the proposal |
|---|---|---|---|
| General comment | Several respondents were concerned that the timing of this consultation could create uncertainty for both competent authorities and CASPs, stating that changes are based on draft legislation and AML/CFT legislation soon to be replaced by draft laws currently in the legislative process. As a consequence, respondents were of the opinion that there is no legal certainty in relation to parts of the consultation that rely on references to legislation that is subject to change, i.e. as long as the legislative process has not been completed and the finalised text published. | The consultation paper reflects the political compromise available at the time. When finalising the guidelines, the EBA adjusted the draft where necessary to reflect the wording of Regulation (EU) 2023/1113 (FTR) that had since been adopted. The EBA did not identify any differences that have a material effect on these guidelines. | None |
| General comment | One respondent, with reference to Directive (EU) 2018/843 ('AMLD5'), is of the view that stringent AML/CFT requirements already apply to a range of crypto-related activities. The respondent also suggests that guidance issued by competent authorities is sufficient and that further EBA guidance is not warranted. | Regulation (EU) 2023/1114 (MiCA) extends the list of services that require an authorisation as a CASP, while Regulation (EU) 2023/1113 extends the definition of 'financial institutions' to include CASPs. This means that, once these regulations apply, all CASPs will be subject to AML/CFT requirements.<br><br>Article 36(3) of Regulation (EU) 2023/1113 provides the EBA with the legal mandate to issue guidelines on the risk-based approach to the AML/CFT supervision of CASPs by competent authorities. These guidelines are addressed to these authorities and serve to foster consistent approaches between supervisors across the EU when designing, implementing, revising and enhancing their AML/CFT risk-based supervision models. National guidelines can complement, but do not replace, EU-level guidelines. | None |
| Impact assessment | One respondent is of the view that the impact of the amending Guidelines in the consultation was not quantified. According to | The EBA considers that costs are arising from legislative changes, in particular the FTR recast and the amendment of Article 3(2) of Directive (EU) 2015/849 for which an impact assessment has already | None |

| | | | |
|---|---|---|---|
| | the respondent, this prevents a full discussion on alternative approaches and how their impacts may differ. | been performed. The amended guidelines merely specify how competent authorities should comply. Section 5.1 of the consultation paper has further details on this point. | |
| **Feedback on responses to Question 1: Do you have any comments on the proposed changes to the 'Subject matter, scope and definitions'?** | | | |
| **Guideline** | **Summary of responses received** | **EBA analysis** | **Amendments to the proposal** |
| Section 'Subject matter, scope and definitions' | One respondent is of the view that the amendment to the FTR creates an uneven playing field for the crypto industry as the nature of competent authorities responsible for the AML/CFT supervision of CASPs varies across Member States. Where competent authorities are FIUs, the respondent considers that it is unclear how the FIUs will implement the guidelines. The respondent therefore believes it might be better not to include a reference to the FTR. | These guidelines are addressed to competent authorities as defined in Article 4 point (2)(iii) of Regulation (EU) No 1093/2010. Competent authorities are required to make every effort to comply with them. Therefore, should an FIU be designated as a competent authority, it should comply with these guidelines when supervising financial institutions as defined in Article 3(2) of Directive (EU) 2015/849. As set out above, Regulation (EU) 2023/1113 extends this definition to CASPs. | None |
| Section 'Subject matter, scope and definitions' | One respondent would like to see crypto-assets-related definitions, or a clear explanation of their source added to the guidelines. Otherwise, the ambiguity of the guidelines level would rise, and their practical input would drop. | Unless otherwise specified, the terms used and defined in Union law, including Directive (EU) 2015/849 and Regulation (EU) 2023/1113, have the same meaning in these guidelines. The EBA, having assessed the consultation response, has amended the relevant paragraph to provide for more clarity. | The definitions section includes a clear reference to relevant legal texts. |
| **Feedback on responses to Question 2: Do you have any comments on the proposed changes to Guideline 4.1. 'Implementing the RBS Model'?** | | | |
| **Guideline** | **Summary of responses received** | **EBA analysis** | **Amendments to the proposal** |
| Guideline 4.1.3. 'Subjects of assessment' | One respondent considers that the EBA should wait for specific guidelines to be issued under MiCAR rather than apply the joint ESMA and EBA 'fit and proper' guidelines and the EBA's Guidelines on internal governance for AML/CFT purposes, as the EBA 'fit and proper' guidelines were not issued having in mind the crypto industry.<br><br>Another respondent agrees that reference should be made to existing EBA guidelines until MiCAR guidelines are in force. They consider this necessary to mitigate potential risk but urge | Since the publication of the consultation version of these guidelines, work on 'fit and proper' guidelines under Regulation (EU) 2023/1114 (MiCA) has begun, and for this reason the EBA has deleted the reference to the joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.<br><br>Based on the responses received, the EBA adjusted the reference to the provisions in Titles II, III, IV and V of the EBA Guidelines on internal | Changes introduced to paragraph 9. |

| | | | |
|---|---|---|---|
| | the EBA to consider whether the 'fit and proper' guidelines and Guidelines on internal governance reflect the operational realities of CASPs and whether the sector would be put at a disadvantage by having to comply with guidelines applicable to traditional service providers.<br>They also welcome further clarity on the extent to which these existing guidelines would be applied to CASPs, taking into consideration their cross-border nature, size, volume, type of activity and internal AML controls. | governance. The reference is now more specific and refers to the EBA Guidelines on internal governance for investment firms. | |
| **Feedback on responses to Question 3: Do you have any comments on the proposed changes to Guideline 4.2. 'Step 1 – Identification of risks and mitigating factors'?** | | | |
| **Guideline** | **Summary of responses received** | **EBA analysis** | **Amendments to the proposal** |
| Guideline 4.2.2. 'Sources of information' | With regard to paragraph 31 letter k) one respondent emphasised that, when utilising blockchain analytics tools, one should never use a single source for blockchain analytics, as the information provided by blockchain analysis tools can vary, and blockchain analysis tools have occasionally been proven to be incorrect. A solution the respondent sees would be to compare the results of blockchain analysis conducted using different analytics tools. | The guidelines set out that competent authorities should identify risk factors in respect of sectors, subsectors, if relevant, and subjects of assessment based on information from a variety of sources. Competent authorities should determine the type and number of these sources on a risk-sensitive basis.<br><br>The EBA agrees that guideline 4.2.2. can be further clarified in this regard and has made amendments to specify that multiple analytics tools should be used as necessary. | Change introduced to paragraph 11. |
| | With regard to paragraph 31 letter k) one respondent underlined the high desire for such a new source of information, however requesting clarification as to the scope of advanced analytics tools and the expected outcomes – is it a report, a file, or maybe an NFT encrypted with the result of the analysis? | Guideline 4.2. sets out that competent authorities should identify and understand the risk factors that will affect each sector's and subject of assessment's exposure to ML/TF risks. For this purpose, and in line with guidelines 4.1.4. and 4.4.9., competent authorities should use different sources of information and actively engage with the sector and with other competent authorities where relevant. Blockchain analytics is one example of advanced analytics tools that could potentially be used. | None |

| | | | |
|---|---|---|---|
| | | Regarding the format and use of the analysis, guideline 4.2. specifies that the information gathered from the sources described in paragraphs 30 and 31 should be sufficient, relevant, and reliable to develop an overall understanding of the inherent risk factors and factors that mitigate these risks within the sector and subsector, where relevant, and – based on the sectoral risk assessment – an overall understanding of the subjects of assessment's inherent risk factors, and, to the extent possible, residual risk factors. | |
| | One respondent suggested adding clarifications to paragraph 31 letter k) and paragraph 45 letter a) as to how competent authorities' access to analytics tools/platforms data is to be established and maintained. The respondent mentions that the current wording does not provide sufficient information on whether, for example, CASPs will be expected to pass on information about analyses that are carried out in relation to them or their customers, or whether (as is currently more common practice) competent authorities would be expected to contract with blockchain analytics firms to obtain analyses directly. | It is for the competent authorities to decide on a risk-sensitive basis how to establish and maintain access to analytics tools data. | None |
| Guideline 4.2.5. 'Sector-wide ML/TF risk factors' | One respondent mentioned that it would be prudent to refer to the specific provisions on obliged entities in Directive (EU) 2015/849 instead of also listing the obliged entities currently mentioned in paragraph 37 of the revised Risk-Based Supervision Guidelines. | The EBA, having assessed the consultation response, amended the relevant paragraph. | Changes introduced to paragraph 12. |
| Guideline 4.2.6. 'Type of information necessary to identify risk factors' | Two respondents commented that it was important that the implications of the technology for ML/TF risks are identified and understood. One respondent mentions that it is important to indicate that there are choices about how technology is used which impact the business model and the ML/TF risk. One approach would be to incorporate specific examples – such as the choice between permissioned and permissionless ledgers or the use of mixers to disguise the origin of coins in a transaction. | The EBA, having assessed the consultation responses, amended the relevant paragraph. | Changes introduced to paragraph 14. |

| | | | |
|---|---|---|---|
| | Another approach would be to amend the draft explicitly to reflect the effect of such choices on ML/TF risk exposure. | | |
| | One respondent stated that adding distributed ledger technology (DLT) as one of the sources that authorities should use to develop a good understanding of the inherent risk factors within the sectors and subsectors brings up the question as to who will be assessing the risks. | As mentioned in guideline 4.2.6. and in order to develop a good understanding of the inherent risk factors within the sectors and subsectors, competent authorities should obtain information which should include, but not be limited to, the information mentioned in paragraph 41. | None |
| | With regard to the amendment made to paragraph 44 letter c), one respondent believes further clarity is necessary as to the typology of transactions needed for supervisory assessment, e.g. transactions pertaining to particular use cases, transactions between certain parties, etc. The respondent reasoned that further details on this obligation would help avoid potential uncertainties and would ensure this piece of information is actually useful and effective for understanding and monitoring inherent risk factors on the side of the competent authority, and for understanding compliance obligations from the side of the CASP. | The Risk-Based Supervision Guidelines are addressed to competent authorities and apply across all financial services sectors. With the amendment to paragraph 44 point c) the EBA highlights the different types of transactions, such as virtual asset to virtual asset or unhosted wallets transactions and related peer-to-peer transactions, that a competent authority should gather information on from various sources to develop a good understanding of the inherent risk factors applicable to CASPs, without being detrimental to the cross-sectoral applicability of this paragraph. | None |
| | One respondent requested further context on the amendment to paragraph 44 letter f) whereby the business activities not only carried out but also located in high-risk third countries would be considered a factor in risk assessment. In particular, they would appreciate more clarity as to how this amendment could transpose into the compliance procedures for obliged entities in the context of correspondent relationships between CASPs. | The EBA, having assessed the consultation response and to provide for any difficulties in tying CASPs to a geographical location, e.g. if they do not have a clearly defined headquarters or centralised operation, amended paragraph 44 point f) by including a nexus with high-risk third countries.<br><br>For CASPs specifically, the EBA highlights that guideline 8 on correspondent relationships in the EBA's Risk Factor Guidelines provides | Changes introduced to paragraph 15. |

| | | | |
|---|---|---|---|
| | | more clarity on risk factors (e.g. on country or geographical risk factors) and measures alongside those set out in Title I of these guidelines.[17] | |
| **Feedback on responses to Question 4: Do you have any comments on the proposed changes to Guideline 4.3. 'Step 2 – Risk assessment'?** | | | |
| **Guideline** | **Summary of responses received** | **EBA analysis** | **Amendments to the proposal** |
| Guideline 4.3.4. 'Individual risk assessment' | One respondent suggested, to account for the inherently cross-border nature of blockchain technology which might not always allow for sufficient publicly available information or full disclosure of all business activities of a third-country CASP, especially if no business agreement exists, adding to paragraph 59: 'that the AML/CFT systems and controls listed in Article 8(4) and, provided that this is feasible, 19a of Directive (EU) 2015/849 are put in place and applied. These controls should be sufficiently comprehensive and commensurate with the ML/TF risks.'<br>The respondent also recommended that competent authorities consider the involvement of reputable third-party providers, i.e. blockchain analytics providers, which have the resources to provide verified risk assessments on on-chain activities and profiling of CASPs around the globe. In this way, competent authorities would be able to more easily conduct their supervisory responsibilities and CASPs would not be subject to an increased administrative burden to collect large quantities of information in relation to correspondent relationships. | Article 8(4) of Directive (EU) 2015/849 and the new Article 19a – which is inserted into Directive (EU) 2015/849 by Article 38(4) of Regulation (EU) 2023/1113 – are legal requirements that financial institutions, including CASPs, must comply with.<br><br>The proposed amendments included by the EBA in guideline 4.2.2. as well as guideline 4.2.6. already cater for the respondent's recommendation. Moreover, the wording in paragraphs 30 and 31 leaves enough room for competent authorities to make use of other sources of information in addition to the ones already mentioned by the EBA. | None |

[17] Consultation Paper on Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849.

| Feedback on responses to Question 5: Do you have any comments on the proposed changes to Guideline 4.4. 'Step 3 – Supervision'? | | | |
|---|---|---|---|
| **Guideline** | **Summary of responses received** | **EBA analysis** | **Amendments to the proposal** |
| Guideline 4.4.2. 'Supervisory Strategy' | With regard to the proposed change to paragraph 78 letter e), one respondent considers that this will require both resources and people, which governments might not currently be able to make available, given the current financial situation and financial stability concerns. Hence, a lack of resources necessary to live up to the proposed change might be an obstacle to consider. | It is the responsibility of Member States to ensure that competent authorities are sufficiently resourced to perform their duties. Competent authorities then have to allocate these resources in a way that enables them to comply with Directive (EU) 2015/849. | None |
| | With reference to paragraph 78 letter e) one respondent deems it appropriate to recommend that, when determining resource needs, authorities take into consideration also possible unplanned off-site/on-site supervisory activities. A sector that is prone to rapid changes is more likely to have occurrences of unplanned inspections. | The EBA agrees with the respondent that so-called contingencies should be part of any supervisory strategy (and an AML/CFT supervisory plan in accordance with paragraph 85). However, this is already included in the current paragraph 78 point f). According to this point a supervisory strategy should explain how competent authorities will tackle and address emerging risks effectively when they arise in a way that does not have an adverse effect on the entire strategy. | None |
| Guideline 4.4.4. 'Supervisory Tools' | One respondent requested clarity on the amendment to guideline 4.4.4.'s section on supervisory tools, whereby 'information from any other relevant authority' is listed as a source of information to substantiate risk assessments. They requested further details as to which other authorities would be considered relevant in this process, for the purposes of providing certainty for CASPs on the monitoring process. | The amendments made to paragraph 94, e.g. the inclusion of information from any other relevant authority, for instance relate to tax authorities, and authorities that are responsible for AML/CFT, conduct and/or prudential supervision of the same subject of assessment, regardless of whether they are domestic authorities, authorities in another Member State or authorities in third countries. The EBA amended the relevant paragraph to provide for more clarity. | Changes introduced to paragraph 19. |
| Guideline 4.4.8. 'Supervisory Follow-up' | With respect to the proposed amendments to paragraph 117, one respondent thinks it would be appropriate to have an explicit reference to supervisory powers that were rarely used or not used at all in the past (removal of directors; prohibition to onboard new clients). The following text was proposed. 'Where competent authorities have suspicions that the failure to implement effective systems and controls may be deliberate, they | Section 4 on sanctions in Directive (EU) 2015/84 is clear on this. Member States shall ensure that obliged entities can be held liable for breaches of national provisions transposing this Directive in accordance with Articles 58 to 61. Any resulting sanction or measure shall be effective, proportionate and dissuasive. Member States shall also ensure that where obligations apply to legal persons in the event of a breach of national provisions transposing this Directive, sanctions and | None |

| | | | |
|---|---|---|---|
| | should consider a more robust follow-up action including the exercise of the power of removal of directors'. | measures can be applied to the members of the management body and to other natural persons who under national law are responsible for the breach. | |
| Guideline 4.4.9. 'Feedback to the sector' | One respondent noted that the new version of paragraph 125's catalogue of guidance indicators is extended by 'concerns about the quality and usefulness of suspicious transaction reports'. However, the new one seems far more concrete compared to other indicators. For example, paragraph 125 letter c) refers to 'evidence of de-risking in some sectors or subjects of assessment, or evidence that subjects of assessment avoid risks rather than manage them effectively'. In that sense, the question of the new indicator's purpose arises. The respondent notes that paragraph 125 contains an open catalogue, which means that the new indicator could have been considered before without any change to paragraph 125. | Competent authorities should assess the need for further guidance in the sector. Information exchange with subjects of assessment is an important tool for competent authorities to assess the level of AML/CFT knowledge and expertise in the sector. As part of this, it is also helpful to bilaterally share, as provided by the FIU to the competent authority, certain risk information, e.g. on the quality and usefulness of suspicious transaction reports, with a subject of assessment.[18] Subjects of assessment can use this information to inform their AML/CFT framework. This is particularly important for new sectors under competent authorities' supervisory remit, such as CASPs. Where such bilateral information exchange on the quality and usefulness of suspicious transaction reports with subjects of assessment cannot take place, this type of information can be a good indicator that may suggest that further guidance may be warranted from the competent authorities. Since new sectors under supervision may struggle with their suspicious transaction reporting obligations, the EBA highlighted this as an important indicator for competent authorities to consider. | None |
| | One respondent noted that it is not clear how concerns about the quality and usefulness of STRs could be an indicator that there might be a need for further guidance. A question also arises with regard to who determines the quality and usefulness of STRs. The respondent states that its members provide suspicious transaction reporting but do not in general receive guidance from the authorities in this respect. It is therefore possible that its members provide very detailed suspicious | Article 32(3) of Directive (EU) 2015/849 states: '*The FIU as the central national unit shall be responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing. The FIU shall be responsible for disseminating the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing*'. This means that the quality | None |

[18] Directive (EU) 2015/849 preamble 49 also mentions that 'feedback on the usefulness and follow-up of the suspicious transactions reports they present should, where practicable, be made available to obliged entities.'

| | | | |
|---|---|---|---|
| | transaction reporting which might not be very useful. Equally, the respondent would like to note that certain of its members recently started to receive feedback on the quality of legitimate STRs from their FIU in some Member States, and the question of how the quality of the STRs is determined becomes in such a context extremely relevant. Furthermore, the respondent would like to note that there are currently no clear boundaries about the extent to which VASPs should conduct the investigation. However, the respondent considers that each investigation should be conducted up to the point where every person reading the STR could draw the same conclusions as the person reporting it. | and usefulness of suspicious transactions reports are primarily determined by the FIU. The FIU's assessment should be used by competent authorities to inform their supervisory work. The reporting of suspicious transactions is an essential obligation of an effective AML/CFT framework. That is why concerns about the quality and usefulness of these reports can impact the resilience of the AML/CFT framework and consequently be an important indicator for the competent authorities that may suggest that further guidance may be warranted. | |
| | One respondent suggested adding an additional point to paragraph 126 letter c) and provided a drafting suggestion to clarify that competent authorities should also cooperate with relevant industry associations when issuing sectoral guidance. This is to ensure that guidance reflects industry views, which is particularly important in a rapidly developing technological environment. | The EBA, after carefully considering the respondent's response, agrees with the fact that competent authorities should also engage with relevant industry associations when issuing guidance to the sector. However, this is already addressed under paragraph 127 in the guidelines, which requires competent authorities to consider engaging with subjects of assessment and other relevant stakeholders – which can include relevant industry associations – when developing supervisory guidance and should determine the most effective way for this outreach. | None |
| Guideline 4.4.10. 'Training of competent authority's staff' | One respondent mentions that it appears appropriate that the monitoring referred to in paragraph 133 is not only about the 'level of training completed' but it also encompasses the quality of the learning. Without this clarification it seems that the focus is on the form (Did he/she attend the training initiatives or not? The question should be: did she/he learn?). | The EBA stresses the importance of training to ensure that staff from competent authorities are well trained and have the technical skills and expertise necessary for the execution of their functions, including the supervision of CASPs. The EBA agrees with the respondent that quality is an important part of any training provided. The EBA notes that this is, however, already covered in the wording of paragraph 133 on the development of a training programme which should be adjusted to meet the needs of specific functions within the competent authority, their job responsibilities, seniority and the experience of | None |

| | | | |
|---|---|---|---|
| | | staff. This training programme should be kept up to date and reviewed regularly, for example where the training received did not bring the desired expertise and results. | |
| | With regard to the changes made to paragraph 133, one respondent considers that the industry should provide guidance to the supervisory authorities on how to use the training material effectively. | The EBA agrees that, where relevant, it may be helpful for competent authorities to engage with relevant (industry) stakeholders when developing a training programme for the competent authority's staff. The EBA amended the relevant paragraph to provide for more clarity. | Changes introduced to paragraph 27. |
| | One respondent states that the newly added paragraph 133A refers to the training of external parties within the authorities' training programme. Yet, the guidelines do not mention the prerequisites of the legitimate usage of the external parties and the scope of their participation in authorities' activities. Does it mean such prerequisites and other rules shall be included in different guidelines, or shall they come from the law applicable to the authorities' actions?<br>In the opinion of another respondent, there should be some guidance from the industry on how this training is done and it might require some time for the competent authorities to provide an analysis that is thorough, based on the training. | Guideline 4.4.7. provides more insight on the use of services of external parties. As the EBA mentioned before, where relevant, it may be helpful for competent authorities to engage with relevant (industry) stakeholders when developing a training programme. | None |
| | One respondent suggested that the provisions on 'technical expertise' could be further strengthened in paragraph 133 by including an explicit reference given the unavoidable need for such expertise in relation to the supervision of CASPs in particular. | The EBA, having carefully considered the respondent's suggestion, thereby balancing legal certainty and keeping the guidelines as future proof as possible, notes that technical expertise includes appropriate technological expertise where intrinsic to the business model, operations or controls of the entities supervised. The EBA therefore finds that no further clarification is necessary at this point. | None |
| | Some respondents commented that, in order to adequately supervise CASPs, the competent authority's staff should be well equipped and trained to understand the relevant technology and the ML/TF implications the technology used by the subject of assessment has, and how to use technology for supervisory purposes. | As mentioned before, the EBA stresses the importance of training to ensure that staff from competent authorities are well trained and have the technical skills and expertise necessary for the execution of their functions, including the supervision of CASPs. | Changes introduced to paragraph 30. |

| | | | |
|---|---|---|---|
| | One respondent suggested adding a new point g) at the end of paragraph 134 as follows:<br>g) understand the technology underpinning business models, operations or controls of supervised entities or supervisory tools sufficiently to assess the risks and controls of supervised entities and to enable the appropriate deployment of technology-enabled supervisory tools. | The EBA, after having carefully considered the respondent's suggestion, agrees that such an addition could be helpful and amended the relevant paragraph. | |
| | One respondent suggests amending paragraph 134 letter c) to state:<br>'including any software or other technological tools used to comply with their AML/CFT obligations.' This is to avoid an unintended wider interpretation of the guideline that would allow competent authorities to also access firms' general software apart from that used for compliance with AML/CFT obligations. | Article 48(2) of Directive (EU) 2015/849 sets out that competent authorities should have adequate powers, including the power to compel the production of any information that is relevant to monitoring compliance and perform checks, and have adequate financial, human and technical resources to perform their functions. This should allow supervisors to request any information or access any system that is relevant to monitoring compliance and perform checks. The proportionality principle as an overarching principle that is applicable to all stages of the supervisory process is set out by the EBA in paragraphs 14 and 15 of the revised Guidelines. This principle should avoid an unintended wider interpretation of the guidelines. It should also be noted that this provision in the guidelines is in the context of training of staff. | None |
| **Feedback on responses to Question 6: Do you have any comments on the proposed changes to Guideline 4.5. 'Step 4 – Monitoring and updating of the RBS Model '?** | | | |
| **Guideline** | **Summary of responses received** | **EBA analysis** | **Amendments to the proposal** |
| Guideline 4.5.1. 'Review of the AML/CFT RBS Model' | One respondent considers that the guidelines should require competent authorities to have professional IT skills and IT training. They consider that it is unclear from the suggested wording whether the term 'technical expertise' encompasses this. | The guidelines provide that competent authorities have the skills necessary to carry out their tasks, including technical expertise. The necessary technical expertise may vary depending on the type of task competent authorities' staff need to perform, such as reviewing and assessing the adequacy and effectiveness of their AML/CFT RBS Model. As a result, technical expertise may include IT expertise. | None |