EBA/GL/2021/16

16 December 2021

Final Report

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 Risk-Based Supervision Guidelines

Contents

Table of Contents

1. Executive Summary **3**

2. Background and rationale **5**

3. Guidelines **12**

Annex **59**

Conversion of risk categories 59

5. Accompanying documents **60**

5.1 Cost-benefit analysis / impact assessment 60

5.2 Feedback on the public consultation and on the response provided by the BSG as part of the consultation 67

Summary of responses to the consultation and the EBA's analysis 69

1. Executive Summary

Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing entered into force on 26 June 2015. The Directive aims, inter alia, to bring European Union legislation in line with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, published by the Financial Action Task Force (FATF), a setter of international standards on anti-money laundering/combating the financing of terrorism (AML/CFT). It puts the risk-based approach at the centre of Europe's AML/CFT regime and recognises that the risk of money laundering (ML) and terrorist financing (TF) can vary. It requires Member States, competent authorities and obliged entities to take steps to identify and assess that risk with a view to deciding how best to manage it.

In accordance with Article 48(10) of Directive (EU) 2015/849, the EBA is required to issue guidelines to competent authorities on the characteristics of a risk-based approach to AML/CFT supervision (RBS). The first iteration of the guidelines was published in 2016 as joint guidelines, as all three European Supervisory Authorities (ESAs) held AML/CFT mandates at the time. They set out steps that supervisors should take when conducting AML/CFT supervision on a risk-sensitive basis. With these guidelines, the ESAs aimed to create a common understanding of the risk-based approach to AML/CTF supervision and to establish consistent and effective supervisory practices across the EU, which are in line with international standards.

There have since been a number of reports that considered the extent to which competent authorities have implemented an effective, risk-based approach to AML/CFT supervision. These include the publication of the EBA's report on competent authorities' approaches to AML/CFT supervision of banks (EBA/Rep/2020/06, the 'EBA report') in February 2020, the publication of the post-mortem report by the European Commission and the publications of the ESAs Joint Opinion on risks under Article 6(5) in October 2019 and March 2021, which all raised concerns about the adequacy and effectiveness of some competent authorities' approaches to the AML/CFT supervision. The EBA assessed these reports and concluded that there was a need for further guidance on this topic to ensure effective AML/CFT supervision going forward. To that end, the EBA concluded that it was necessary to revise the guidelines.

The proposed amendments address the key challenges for supervisors when implementing the risk-based approach. They also take into consideration changes in the EU legal framework that came into force since the guidelines were first issued and new international guidance by the FATF and the Basel Committee on Banking Supervision on this topic. In summary, the revised guidelines:

- emphasise the need for a comprehensive risk assessment at a sectoral and subsectoral level to support competent authorities' identification of those risk areas that require more intense supervisory attention;

- explain different supervisory tools available to competent authorities and provide guidance on selecting the most effective tools for different purposes;

- emphasise the importance of a robust follow-up process and set out different aspects that competent authorities should consider when determining the most effective follow-up action;

- provide further guidance on the implementation of a robust supervisory strategy and plan, to ensure that competent authorities allocate their supervisory resources according to the risk exposure of subjects of assessment under their supervision;

- clarify competent authorities' obligations as regards the AML/CFT supervision of groups and emphasise the need for competent authorities, that are responsible for the supervision of the group's head office, to develop a good understanding of ML/TF risks to which the group is exposed with a view to ensuring that group-wide policies and procedures are implemented effectively;

- highlight the importance of cooperation among competent authorities and between competent authorities and other stakeholders, including prudential supervisors, the financial intelligence unit (FIU), tax authorities, law enforcement and AML/CFT authorities in third countries. In particular, the guidelines recognise that supervisory cooperation is important not only when supervising cross-border groups, but also in respect of domestic groups and subjects of assessments.

- provide further guidance on how competent authorities can determine the type of guidance needed within the sector and how to communicate this guidance in the most effective manner.

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 three months after the publication in the EU official languages.

2. Background and rationale

2.1 Background

1. Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing aims, inter alia, to bring EU legislation in line with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation that the Financial Action Task Force (FATF), an international AML/CFT standard-setter, adopted in 2012.

2. In line with the FATF's standards, the Directive puts the risk-based approach at the centre of Europe's anti-money laundering and countering the financing of terrorism (AML/CFT) regime. It recognises that the risk of money laundering (ML) and terrorist financing (TF) can vary and that Member States, competent authorities and obliged entities have to take steps to identify and assess that risk with a view to deciding how best to manage it. Consequently, under a risk-based approach, competent authorities should allocate their AML/CFT supervisory resources in a risk-sensitive way in order to exercise their responsibilities more effectively.

3. Directive (EU) 2015/849 requires competent authorities to monitor effectively, and to take the measures necessary to ensure compliance with the Directive. As part of this, it requires competent authorities to adjust the frequency and intensity of onsite and offsite supervision to reflect the outcomes of their ML/TF risk assessments. In accordance with Article 48(10) of Directive (EU) 2015/849, the EBA is required to issue guidelines to competent authorities on the characteristics of a risk-based approach to AML/CTF supervision.

4. To that end, the 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 (ESAs 2016 72) under Article 48(10) of the Directive (EU) 2015/849 (the 'Original Guidelines') were first published on 16 November 2016 as joint guidelines, as all three European Supervisory Authorities (ESAs) held AML/CFT mandates at the time. In the Original Guidelines, the ESAs characterised the risk-based approach to AML/CFT supervision as an ongoing and cyclical process that consists of four steps, namely the identification of ML/TF risk factors; the assessment of ML/TF risks; the allocation of AML/CFT supervisory resources based on the outcomes of this risk assessment, including decisions on the focus, depth, duration and frequency of onsite and offsite inspections, and on supervisory staffing needs; and the monitoring and review of their risk-based supervision model, including the risk assessment and the underlying methodology. With these Original Guidelines, the ESAs aimed to create a common understanding of the risk-based approach to AML/CTF supervision and to establish consistent and effective supervisory practices across the EU, which are consistent with international standards. All competent authorities indicated that they complied, or intended to comply, with the Original Guidelines.

5. Since then, reviews of competent authorities' implementation of the Original Guidelines and their compliance with the underlying legal obligations have identified that supervisors are finding it challenging to translate their theoretical understanding of the risk-based approach into practice. The reviews found that as a result, AML/CFT supervision of credit institutions and financial institutions in the EU was not always adequate or effective. These reports include:

   - Mutual Evaluation Reports by the FATF and Moneyval that have highlighted various shortcomings in the AML/CFT supervisory framework in some Member States. By February 2021, 15 out of 20 Member States that had been assessed in recent years were found to be 'moderately effective' in their AML/CFT supervision, with only 2 Member States assessed as having a 'substantive' level of effectiveness and 3 Members States as having a low level of effectiveness.

   - The EBA's report on competent authorities' approaches to AML/CFT supervision of banks[1] (the 'EBA Report') published in February 2020, which highlighted that competent authorities' approaches to identifying and assessing ML/TF risk associated with the sector, and the ML/TF risk associated with individual banks under their supervision were often inadequate. This meant that often competent authorities in the EBA's sample were unable to target their supervisory resources on areas presenting the greatest ML/TF risk in their jurisdiction. In addition, some supervisors found it challenging to implement an effective supervisory strategy and plan, which meant that they did not supervise firms in a strategic or consistent way, with institutions in some sectors not being supervised at all.

   - The ESAs' Joint Opinion on ML/TF risks published in accordance with Article 6(5) of Directive (EU) 2015/849 in October 2019, identified significant differences in the way the risk-based supervision was carried out by competent authorities across the EU. The ESAs considered that these differences may have significant implications for the robustness of the EU's AML/CFT defences and for the integrity and stability of the overall financial sector. The ESAs explained that, based on information received from competent authorities, it was evident that most competent authorities focused their attention on sectors they considered to present significant ML/TF risks, while applying very little or no supervision to sectors perceived to be less risky. In this opinion, the ESAs also raised concerns about the quality and adequacy of risk assessments carried out by competent authorities, as they found that in some instances the assessment was based solely or largely on one risk factor.

   - The European Commission's post-mortem report on the assessment of recent alleged money laundering cases involving EU credit institutions[2] that was published on 24 July 2019 and in which the Commission identified many failures by competent authorities in the way they had supervised banks involved in recent money laundering scandals. Overall, the report highlights that in most cases competent authorities had failed to identify risks and had failed to choose adequate tools to supervise those risks and to apply robust supervisory measures when breaches were identified.

[1] EBA's report on competent authorities' approaches to AML/CFT supervision of banks, EBA/Rep/2020/06.

[2] European Commission's Report on the assessment of recent alleged money laundering cases involving EU credit institutions, COM(2019) 373 final.

- The EBA published a report on competent authorities' approaches to tackling ML/TF risk associated with illicit dividend arbitrage trading schemes and found that not all competent authorities had the same understanding of dividend arbitrage trading schemes, due to differences in Member States' domestic tax laws, which meant that proper considerations were not given to incorporating risk associated with tax crimes in the competent authorities' risk assessments. The EBA also adopted a cum-ex action plan[3] in April 2020, where it recommended the that the Risk-based Supervision Guidelines include additional requirements on how AML/CFT competent authorities should identify, assess and address ML/TF risks associated with tax crimes and clarify how AML/CFT supervisors and tax authorities should cooperate, in line with changes introduced by Directive (EU) 2018/843.

- The European Council's AML/CFT Action plan published in December 2018 identified a number of shortcomings in supervisors' approaches to tackling ML/TF risk and called on the EBA's action to strengthen AML/CFT supervision in the EU, including by revising the ESAs Risk-based Supervision Guidelines.

6. Against this background, the EBA concluded that there was a need for further guidance on this topic to ensure effective AML/CFT supervision going forward by making changes to the existing ESAs Risk-based Supervision Guidelines. The revised guidelines build on the existing 4-step approach to the supervision and enhance the existing or introduce additional guidance on aspects that have been identified as causing the most challenges for competent authorities as set out below. The revised guidelines take into account the recent international guidance in the area of AML/CFT, including the development of guidance on risk-based supervision by the FATF and the existing Basel Committee guidelines on this topic.

7. In addition, the revised guidelines address changes introduced by Directive (EU) 2018/843, which entered into force on 9 July 2018 and amended Directive (EU) 2015/849, whereby the directive highlights the need for cooperation between competent authorities and with other stakeholders, including prudential supervisors and financial intelligence units. To that end, the revised guidelines recognise the links with other EBAs and the ESAs' guidelines, including the ESAs Joint Guidelines on Cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions (JC 2019 81) and the EBA's Guidelines on Cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Article 117(6) of Directive 2013/36/EU.[4]

8. Furthermore, the revised guidelines aim to address concerns raised in response to the EBA's Call for Input on de-risking,[5] which aimed to develop a better understanding of the impact of de-risking on credit and financial institutions and on individuals, by explaining what competent authorities should do to reduce unwarranted de-risking of current and potential customers by some sectors.

---

[3] EBA's Action plan on dividend arbitrage trading schemes ('Cum-Ex/Cum-Cum'), April 2020.

[4] EBA Guidelines on Cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Article 117(6) of Directive 2013/36/EU, December 2021

[5] EBA Call for input on 'de-risking' and its impact on access to financial services, Summer 2020.

9. The EBA publicly consulted on a draft version of these guidelines between 17 March 2021 and 17 June 2021. A public hearing took place on 22 April 2021. The Consultation Paper (EBA/CP/2021/11) included a number of specific questions for respondents to consider. The EBA received ten responses, including a response from the EBA's Banking Stakeholders' Group (BSG). The Feedback Table in Chapter 5.2. provides an overview of consultation responses received by the EBA, with the EBA's assessment, and explains the changes that the EBA decided to make to the draft guidelines as a result.

10. The Original Guidelines will be repealed and replaced with the revised guidelines.

2.2 Rationale

11. This chapter explains the rationale for the key amendments and additions that the EBA made to the original version of the guidelines to address the new EU legislative framework and new risks. However, the key principles underlying the Original Guidelines have not changed:

- The revised guidelines have not made changes to the basic concepts and a 4-step approach to supervision developed by the ESAs in the Original Guidelines, which consist of the identification of ML/TF risk factors, assessment of the ML/TF risks, supervision of obliged entities and sector and monitoring and review of the risk-based supervision model. This means that the risk-based supervision should be based on the ML/TF risk assessment carried out by competent authorities.

- The guidelines acknowledge that some credit institutions and financial institutions may share the same characteristics and level of risk. This means that it may be more effective to treat these credit institutions and financial institutions by competent authorities as one subject of assessment.

- The guidelines recognise that the same level and intensity of supervision is not required in respect of all credit institutions and financial institutions and that supervision should be adjusted in line with the ML/TF risk exposure of the sector and subjects of assessment.

- The guidelines recognise the national differences when transposing Directive (EU) 2015/849 into their national laws, which means that a complete convergence in terms of supervision across the EU is not always possible.

Amendments to the 'Subject matter, scope and definitions'

12. The revised guidelines made various non-substantive changes to the 'Subject matter, scope and definitions' section to align the Original Guidelines, which were developed by the Joint Committee of three ESAs, with the EBA's drafting requirements.

13. In addition, the EBA revised a number of definitions of the Original Guidelines and added new ones, as follows:

a) The definition of 'cluster' has been revised to clarify that competent authorities may decide to treat two or more credit institutions or financial institutions as one cluster where those credit or financial institutions share similar characteristics and are exposed to the same levels of ML/TF risk. The EBA has removed a reference to 'group of subjects of assessments' from the definition of 'cluster' to clarify that the cluster can be treated as a subject of assessment as set out in the definition of 'subjects of assessment'.

b) The definition of 'competent authority' was removed as it was deemed redundant in light of the inclusion of a new section titled 'Addressees' in the guidelines, which clearly sets out who the competent authorities are.

c) The definition of 'firm' has been replaced throughout the guidelines with 'credit institutions and financial institutions' as this term is defined in Directive (EU) 2015/849.

d) The definition of 'inherent money laundering / terrorist financing ('ML/TF') risk' has been amended so that it refers to the 'inherent risk'. In addition, the definition clarifies that the inherent risk refers to the ML/TF risk in the subject of assessment and sector before the application of the mitigating measures.

e) In the definition of 'risk-based approach (RBA)', the term 'obliged entities' has been replaced with 'subjects of assessment' to reflect the notion of clusters that imply that some 'obliged entities' can be grouped together when applying the RBA.

f) The definition of 'risk-based AML/CFT supervision (RBS)' has been removed as it is described in detail in these guidelines and in Directive (EU) 2015/849.

g) In the definition of 'RBS Model' the reference to practicalities has been removed as the definition already contains references to 'processes and procedures'.

h) The definition of 'ML/TF risk' has been revised to avoid duplication with a separate definition that defines the term 'inherent risk'.

i) The definition of 'risk profile' has been revised to clarify that the risk profile may be developed for subjects of assessment and also for sectors/subsectors. The definition also clarifies that the risk profile is not limited only to the residual risk, as it was suggested in the existing guidelines, but may also be based on inherent risk, where, for example, the information on mitigating measures is not available to the competent authority at the time.

j) The definition of 'subject of assessment' has been revised by removing a reference to sectors and subsectors in order to distinguish the steps that should be taken by competent authorities in respect of sectoral and subsectoral risk assessments from the step they should take in respect of credit and financial institutions. A reference to 'group' was removed from the definition to avoid possible confusion with the concept of 'clusters'.

k) The definition of 'threat' was adjusted slightly to remove the general explanation of what is a threat and to make it more relevant for the application in an AML/CFT environment. Also, a reference to 'their funds' was removed from the definition.

l) Definitions of 'ad hoc inspection', 'AML/CFT returns', 'follow-up inspection', 'full-scope on-site inspection', 'off-site review', 'emerging risk', 'de-risking', 'residual risk', 'supervisory tools', 'thematic inspection' have been added to the guidelines. Definitions of these terms were deemed necessary to foster convergence of approaches by competent authorities as all these terms are widely but inconsistently used by competent authorities across the EU.

Amendments to Guideline 4.1: Implementing the RBS Model

14. In accordance with the Original Guidelines, competent authorities are required to implement a supervisory model, which is based on their risk assessment of sectors and subjects of assessment. The risk-based supervision model (the RBS model) involves four steps: the identification of risk factors, the assessment of the ML/TF risks, the supervision of subjects of assessment and the monitoring and review of the model. However, the EBA Report recognised that some of these steps were interpreted and applied inconsistently by competent authorities across the EU when trying to implement them in practice. Therefore, the revised guidelines set out additional guidance for competent authorities on each of the steps to ensure that the RBS Model is developed and implemented effectively across all sectors and across the EU.

15. In addition, the guidelines have been revised to emphasise the importance of cooperation among competent authorities and with other authorities responsible for the supervision of credit and financial institutions. This follows the European Commission's Post-Mortem Report, which identified limited cooperation between competent authorities and with prudential supervisors as one of the factors contributing to the various failures to implement robust AML/CFT frameworks by some of the European banks.

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

16. As set out in the Original Guidelines, in order to implement their RBS Model, competent authorities should start with identifying risk factors that affect their sectors and subjects of assessment. To inform their view of the relevant risk factors, competent authorities should refer to the EBA's AML/CFT Risk Factors Guidelines[6]. However, the EBA report identified weaknesses in this process, in particular that most competent authorities were using the same set of risk factors for all banks and, in some cases, for all financial institutions. In addition, as highlighted by both, the report and the 2019 Opinion on ML/TF risk, most competent authorities had not carried out the assessment of ML/TF risks at a sector level, which meant that their understanding of the risk factors associated with subjects of assessment was often inaccurate and did not appear to represent the current situation within the Member State. Therefore, the revised guidelines provide further clarifications on the need for sectoral risk assessments and the type of information and sources of information that competent authorities should use to identify the risk factors within sectors and subjects of assessment.

Amendments to Guideline 4.3: Step 2 – Risk assessment

17. In line with Article 48(6) of Directive (EU) 2015/849, competent authorities are obliged to have a clear understanding of the ML/TF risk present in their Member States. Competent authorities' risk assessment then forms the basis for competent authorities' risk-based approach.

18. It is evident that competent authorities are at different maturity levels in terms of their risk assessments and, while most competent authorities assessed by the EBA as part of its

[6] Consultation Paper on the draft guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 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 (JC 2019 87)

implementation reviews were striving to implement a robust risk assessment process, many found it challenging to incorporate the risk factors identified by them in their supervisory risk assessments.

19. To that end, the revised guidelines set out the main components of a risk assessment. For clarity purposes and in order to emphasise the importance of the sectoral risk assessment, the revised guidelines make a clear distinction between individual risk assessments of subjects of assessment and sectoral/ subsectoral risk assessments. The guidelines also introduced a requirement for competent authorities to develop a good understanding of ML/TF risks associated with the group.

Amendments to Guideline 4.4: Step 3 – Supervision

20. In line with the FATF guidance, a risk-based approach to supervision involves tailoring the supervisory actions and response to address the specific risks within the sector or subjects of assessment. This approach allows supervisors to allocate resources effectively and focus on higher risk areas.

21. The EBA report highlights that competent authorities were finding it challenging to translate the theoretical knowledge of ML/TF risks into supervisory practice and risk-based supervisory strategies. The report also refers to competent authorities' failures to assess the effectiveness of AML/CFT systems and controls put in place by financial institutions, rather than merely test the institution's compliance with a prescriptive set of AML/CFT requirements.

22. To that end, the guidelines have been revised to address weakness identified by FATF and the EBA related to the risk-based supervision in the EU.

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

23. The guidelines set out that in the final step of the RBS Model, competent authorities are required to review their approach, including their risk assessments and their methodology, and their supervisory strategy and plans. As a result, if inconsistencies or weaknesses are identified, the guidelines require competent authorities to make adjustments where necessary.

3. Guidelines

EBA/GL/2021/16

16 December 2021

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 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[7]. 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 06.06.2022. 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/2021/16'. 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 the EBA.

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

[7] 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

Subject matter

5. These guidelines specify in accordance with Article 48(10) of Directive (EU) 2015/849[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.

Scope of application

6. Competent authorities should apply these guidelines when designing, implementing, revising and enhancing their own AML/CFT risk-based supervision model (RBS Model).

Addressees

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

Definitions

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

Ad hoc inspection	means a review that is triggered by a specific event or ML/TF risk
AML/CFT returns	means regular or ad hoc requests by competent authorities to subjects of assessment for quantitative or/and qualitative data and information relating to key ML/TF risk indicators.
Cluster	means two or more credit institutions or financial institutions in a sector having similar characteristics and exposure to the same levels of ML/TF risk.
De-risking	means a refusal to enter into, or a decision to terminate, business relationships with individual customers or categories of customers associated with higher ML/TF risk, or to refuse to carry out higher ML/TF risk transactions.

[8] 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).

Emerging risk	means a risk that has never been identified before or an existing risk that has significantly increased.
Follow-up inspection	means a review, which serves to assess whether weaknesses in subject of assessment's AML/CFT systems and controls framework identified during a previous inspection or review have been corrected.
Full-scope on-site inspection	means a comprehensive review of all AML/CFT systems and controls implemented by subjects of assessment or their business lines, which takes place on the premises of subject of assessment.
Inherent risk	refers to the level of ML/TF risk present in a subject of assessment or a sector before mitigating measures are applied.
ML/TF Risk	means the likelihood and impact of ML/TF taking place.
ML/TF risk factors	means variables that, either on their own or in combination, may increase or decrease ML/TF risk.
Off-site review	means a comprehensive review of subjects of assessment's AML/CFT policies and procedures, which is not taking place on the premises of subjects of assessment.
Risk-based approach (RBA)	means an approach whereby competent authorities and subjects of assessment identify, assess and understand the ML/TF risks to which subjects of assessment are exposed and take AML/CFT measures that are proportionate to those risks.
RBS Model	refers to the whole set of procedures, processes and mechanisms that competent authorities use to exercise their AML/CFT supervisory powers in a way that is commensurate with the identified ML/TF risks.
Residual risk	means the level of risk that remains after AML/CFT systems and controls are applied to address the inherent risk.
Risk profile	refers to the overall characteristics of the ML/TF risk associated with the subject of assessment or sector/sub-sector, including the type and level of risk.
Subject of assessment	means a credit institution or a financial institution or a cluster, categorised according to criteria laid down by the competent authorities.

Supervisory tools	means all supervisory measures competent authorities can take to ensure compliance by subjects of assessment with their AML/CFT obligations.
Thematic inspection	means a review of a number of subjects of assessments that focus on one specific or very few aspects of these subject of assessments' AML/CFT systems and controls.
Threat	means the potential harm caused by criminals, terrorists or terrorist groups and their facilitators, through their past, present and future ML or TF activities.

3. Implementation

Date of application

9. These Guidelines will apply three months after publication in all EU official languages [04.07.2022].

Repeal

10. The following guidelines are repealed with effect from the date of application.

    Joint 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 (ESAs/2016/72).

4. Guidelines

4.1 Implementing the RBS Model

4.1.1 General considerations

11. Competent authorities should apply the following four steps as part of an effective AML/CFT RBS Model:

    a) Step 1 – Identification of ML/TF risk factors;

    b) Step 2 – Risk assessment;

    c) Step 3 – AML/CFT Supervision; and

    d) Step 4 – Monitoring and review of the RBS Model.

12. Competent authorities should take into account that the risk-based supervision is not a one-off exercise, but an ongoing and cyclical process.

13. Competent authorities should implement the general considerations set out in paragraphs 11 and 12 of these guidelines throughout their RBS model.

4.1.2 Proportionality

14. Competent authorities should be proportionate in their supervision of subjects of assessment for AML/CFT purposes. The extent of information sought, and the frequency and intensity of supervisory engagement and dialogue with a subject of assessment should be commensurate with the ML/TF risk identified.

15. Competent authorities should recognise that the size or systemic importance of a subject of assessment may not, by itself, be indicative of the extent to which it is exposed to ML/TF risk; small credit institutions or financial institutions that are not systemically important can nevertheless pose a high ML/TF risk.

4.1.3 Subjects of assessment

16. Competent authorities should identify those credit institutions or financial institutions within each sector that share a sufficient amount of similar characteristics to justify being grouped in one cluster. The shared characteristics should include the same level of risk that they are exposed to, inter alia, their size, the nature of their business, the type of customers serviced, the geographic area they operate in or activity and their delivery channels. For clustered credit institutions or financial institutions, the RBS process may be carried out at the collective level of the cluster itself, rather than at the level of each individual credit institution or financial institution within that cluster.

17. In order to identify those credit institutions or financial institutions that may belong to the same cluster, competent authorities should refer to their business model, the sectoral risk assessment, the risk assessments of individual credit institutions or financial institutions as well as other relevant sources of information as set out in paragraphs 30 and 31 of these guidelines, including the information gathered as a result of their supervisory activities.

18. Competent authorities should consider whether they will treat credit institutions or financial institutions in the same sector that form part of the same domestic financial group as one 'subject of assessment'.

19. 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, as assessed in line with the Joint ESMA and EBA 'Fit and Proper' Guidelines[9] or because the credit institution's or financial institution's internal control framework is deficient as assessed in line with the EBA's internal Governance Guidelines,[10] which has an impact on the credit institution's or financial institution's residual risk rating, or because the credit institution or financial institution has introduced significant changes to its 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.

4.1.4 Cooperation

20. Competent authorities should cooperate and exchange all relevant information with each other and with other stakeholders, including prudential supervisors, financial intelligence units, tax authorities, law enforcement agencies, judicial authorities and AML/CFT supervisors of third countries to ensure the effective AML/CFT supervision of subjects of assessment. All relevant information should be exchanged without delay. Where subjects of assessment operate on a cross-border basis, such cooperation should extend to competent authorities of other Member States and where relevant, competent authorities of third countries.

21. In order to cooperate and exchange information effectively, competent authorities should apply all cooperation and coordination measures and tools at their disposal, including those competent authorities have been required to put in place in accordance with Directive (EU) 2015/849. Competent authorities should ensure the reliability and continuity of these measures and tools to minimise the risk of a potential information void. In particular, competent authorities should refer to the ESAs Joint guidelines on cooperation and information

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

exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions, [11] the EBA Guidelines on cooperation and information between prudential and AML/CFT supervisors and financial intelligence units under Directive (EU) 2019/878 [12] and the Multilateral Agreement between the European Central Bank and national competent authorities pursuant to Article 57a(2)(b) of Directive (EU) 2015/849.[13]

22. Competent authorities should consider the extent and objective of their cooperation and information exchange with other stakeholders, which may determine the most effective way for this cooperation, as the same approach may not be suitable in all circumstances. This means that more frequent cooperation and exchange of information may be necessary with other competent authorities and prudential supervisors, which are involved in the supervisor of the same subject of assessment, than with financial intelligence units, tax authorities and law enforcement agencies.

23. When cooperating and exchanging information with other stakeholders, including law enforcement agencies, tax authorities, and other bodies or agencies, competent authorities should do so to the extent possible under national law. Competent authorities should seek to exchange information with local tax authorities on various tax offences and mechanisms, which would help the competent authority to assess the resulting ML risks to which the subjects of assessment or sectors may be exposed. It may also exchange information on possible preventative actions in this area.

4.2 Step 1 – Identification of risk and mitigating factors

4.2.1 General considerations

24. Competent authorities should identify and understand the risk factors that will affect each sector's and subject of assessment's exposure to the ML/TF risks. For this purpose, competent authorities should use different sources of information provided in Guideline 4.2.2 and also actively engage with the sector and with other competent authorities where relevant, as set out in Guidelines 4.1.4. and 4.4.9.

25. When identifying ML/TF risk factors, competent authorities should draw on the EBA's ML/TF risk factors guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated

[11] Joint guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions, 'The AML/CFT Colleges Guidelines', JC 2019 81.

[12] EBA Guidelines on Cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Article 117(6) of Directive 2013/36/EU, December 2021

[13] Multilateral Agreement between the European Central Bank and national competent authorities pursuant to Article 57a(2)(b) of Directive (EU) 2015/849.

with individual business relationships and occasional transactions under Articles 17 and 18(4) of Directive (EU) 2015/849.[14]

26. Where subjects of assessment are clusters, competent authorities should identify relevant factors based on those listed in paragraphs 44 and 45 to characterise the cluster as a whole. This should enable competent authorities to justify their decisions on the risk profile they assign to the cluster. Competent authorities should also consider the results of previous supervisory actions in respect of subjects of assessment included within that cluster.

27. Where a subject of assessment is supervised by multiple competent authorities within one Member State, those competent authorities should cooperate and exchange information on that subject of assessment in order to develop a common understanding of its risk exposure.

28. The extent and type of information sought by competent authorities to identify risk factors and mitigating factors should be proportionate to the nature and size, where known, of the subjects of assessment's business activities. It should also take into account the subjects of assessment risk profile as determined on the basis of previous risk assessments, if any, and the context in which the subject of assessment operates, such as the nature of the sector to which the subject of assessment belongs. Competent authorities should consider setting out:

    a) what information they will always require in respect of subjects of assessment and require similar information for comparable subjects of assessment;

    b) where and how they will obtain this information; and

    c) the type of information which will trigger a more extensive and in-depth information request.

4.2.2 Sources of information

29. 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. Competent authorities should ensure that they have access to appropriate sources of information and take steps, where necessary, to improve these. Competent authorities should also ensure that they have implemented processes and procedures for collecting the necessary data.

30. The sources of information that competent authorities should always consider include:

    e) the European Commission's supranational risk assessment published in accordance with Article 6(1) of Directive (EU) 2015/849;

    f) the EBA's Opinion on the ML/TF risk affecting the Union's financial sector published in

[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.

accordance with Article 6(5) of Directive (EU) 2015/849;

g) the national risk assessment (NRA) of the Member State and other Member States as referred to in Article 7(1) of Directive (EU) 2015/849;

h) Delegated Acts adopted by the European Commission as referred to in Article 9(2) of Directive (EU) 2015/849;

i) national and foreign governments;

j) outcomes of the EBA's risk assessments as referred to in Article 9a of Regulation (EU) No 1093/2010;

k) other competent authorities;

l) AML/CFT supervisory authorities in third countries;

m) supervisory authorities responsible for the supervision of subjects of assessment's compliance with prudential requirements, including competent authorities as defined in points (2)(i) and (viii) of Article 4 of Regulation (EU) No 1093/2010, points (2)(i) of Article 4 of Regulation (EU) No 1094/2010, and points (3)(i) of Article 4 of Regulation (EU) No 1095/2010;

n) the financial intelligence units (FIUs);

o) law enforcement agencies, where not excluded by the applicable law;

p) tax authorities, where not excluded by the applicable law; and

q) AML/CFT colleges, established in accordance with the ESAs' Joint Guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions (the AML/CFT Colleges Guidelines')[15], where established.

31. Other sources of information competent authorities should also consider include:

a) the EBA's AML/CFT central database as referred to in Article 9a (1) and (3) of Regulation (EU) No 1093/2010, when the information is made available to the competent authority;

b) colleges of prudential supervisors, set up in line with Article 51 or 116 of Directive (EU) 2019/878 and with the Commission Implementing Regulation (EU) 2016/99 of 16 October 2015 on the operational functioning of colleges of supervisors, and the Commission Delegated Regulation (EU) 2016/98 of 16 October 2015 on the general conditions for the functioning of colleges of supervisors, where established;

c) industry bodies, including information gathered as part of public-private partnerships, if available, such as typologies and information on emerging risks;

d) civil society such as corruption perception indices;

[15] ESAs Joint Guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions (JC 2019 81)

e) international or supranational standard-setting bodies such as mutual evaluations of countries' AML/CFT, anti-corruption and tax regimes;

f) information from credible and reliable open sources, such as reports in reputable newspapers;

g) reputable commercial organisations such as risk and intelligence reports;

h) whistleblowing reports;

i) information from academic institutions; or

j) external auditors' reports in respect of the subject of assessment, where they are available.

4.2.3 Domestic risk factors

32. Competent authorities should have adequate knowledge, awareness and understanding of the ML/TF risks identified at the national level in order to identify the ML/TF risk factors associated with the domestic activities of subjects of assessment and within sectors.

33. As part of this, and based on the sources described in paragraphs 30 and 31, competent authorities should understand, among other things:

a) the type, typologies and scale of money laundering linked to predicate offences, including but not limited to tax offences, committed domestically;

b) the scale of laundering of proceeds from predicate offences, including but not limited to tax offences, committed abroad;

c) the type, typologies and scale of terrorism financing and the scale and the level of support for terrorist activities and groups in the country;

d) relevant ML/TF typologies identified by the FIU and other public authorities or relevant credible private bodies.

4.2.4 Foreign risk factors

34. Where a subject of assessment or a sector as a whole maintains significant links with other Member States or third countries so that the subject of assessment or sector is exposed to ML/TF risks associated with these other countries, competent authorities should identify these risks. Significant links include those where:

a) a subject of assessment maintains a significant level of business relationships with customers from other Member States or third countries;

b) a beneficial owner of a customer of the subject of assessment is from other Member States or third countries;

c) a subject of assessment is carrying out significant levels of occasional transactions with

other Member States or third countries;

d) a subject of assessment maintains significant business relationships with counterparties established in other Member States or third countries;

e) a subject of assessment forms part of a financial group established in another Member State or third country;

f) a subject of assessment's beneficial owners are based in another Member State or third country;

g) a subject of assessment's managing body is comprised of individuals from another Member State or third country; and

h) a subject of assessment has any other relevant links to another Member State or third country, which means that it is exposed to the ML/TF risk associated with that country.

35. Competent authorities should take reasonable steps to acquire and keep up to date adequate knowledge, awareness and understanding of the ML/TF risks associated with these Member States or third countries that may affect the activities carried out by the subjects of assessment. To this end, competent authorities should identify risk factors in line with the EBA's AML/CFT Risk Factors Guidelines[16] and those described in paragraphs 33 and 34 above for each of these Member States or third countries.

36. When identifying third countries which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the European Union, competent authorities should have regard to the delegated acts adopted by the European Commission in accordance with Article 9(2) of Directive (EU) 2015/849 as well as public statements issued by relevant international standard-setters, including the Financial Action Task Force (FATF), the European Council's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) or other FATF-style regional bodies (FSRBs).

4.2.5 Sector-wide ML/TF risk factors

37. 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 refer to the categories of obliged entities listed in Directive (EU) 2015/849, which are credit institutions, credit providers (other than credit institutions, for example consumer credit, factoring, leasing, mortgage credit and commercial credit), life insurance undertakings, life insurance intermediaries, e-money

[16] 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.

institutions, payment institutions, 'bureaux de change', investment firms and collective investment undertakings.

38. 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. Subsectors may include money-remitters, private banks, and brokerage firms, which represent subsectors of payment institutions, credit institutions and investment firms, respectively. To inform their view on sectors and subsectors and their specific features, competent authorities should refer to the Title II of the EBA's AML/CFT Risk Factors Guidelines.[17]

39. Competent authorities should understand how each sector and subsector is organised, and the risks associated with shared features such as the type of products and services offered, the delivery channels used and the type of customers they service. Competent authorities should base their understanding of the sectoral and subsectoral risk factors on:

    a) a high-level view of all relevant information related to subject of assessment in a particular sector or subsector as set out in paragraphs 44 and 45 in these guidelines in order to identify commonalities within each sector and subsector as a whole; and

    b) relevant information related to the sectors and subsectors as set out in paragraphs 41 in these guidelines.

4.2.6 Type of information necessary to identify risk factors

a. Information on sectors

40. Competent authorities should gather sufficient, relevant and reliable information from the sources described in paragraphs 30 and 31 to develop an overall understanding of the inherent risk factors and factors that mitigate these risks within the sector and subsector, where relevant.

41. 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:

    c) information on the size, scope of activities, and complexity of the sector in an aggregated format;

    d) the nature of the business models within the sector;

[17] 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.

e) general information on the type of products, services, customers and delivery channels used within the sector or subsector and their risk profiles, if known;

f) information on the current and emerging risks associated with the sector or subsector domestically and internationally, including the information that may indicate that the sector or subsector may be exposed to increased ML/TF risk as a result of de-risking practices applied to these sectors or subsectors by other sectors;

g) information on the main ML/TF risks affecting the internal market;

h) the impact of cross-border activities within the sector or sub-sector;

i) the sector's or subsector's exposure to vulnerabilities that arise in a global context;

j) threat reports, alerts and typologies from the financial intelligence unit and other relevant state bodies, if applicable; and

k) guidance published by other competent authorities or international standard-setters;

42. The information described above can also contribute to the competent authorities' perception of risk factors on the level of individual subjects of assessment and vice versa.

b. Information on subjects of assessment

43. Based on the sectoral risk assessment, competent authorities should gather sufficient, relevant and reliable information from the sources described in paragraphs 30 and 31 to develop an overall understanding of the subjects of assessment's inherent risk factors, and, to the extent possible, residual risk factors.

44. In order to develop a good understanding of the inherent risk factors applicable to subjects of assessment, competent authorities should gather information from various sources that includes, but is not limited to, the information relating to:

a) the ownership and corporate structure of the subjects of assessment, taking into account whether the subject of assessment is a foreign or domestic credit institution or financial institution, parent company, subsidiary, branch or other kind of establishment, and the level of complexity and transparency of its organisation and structure;

b) the reputation and integrity of senior managers, members of the management body and qualifying shareholders;

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

d) the delivery channels used, including the provision of services through non-face-to-face channels and the use of agents or intermediaries;

e) the types of customers serviced by the subject of assessment and the level of risk associated with those customers, including customers that are politically-exposed persons (PEPs) and those assessed as presenting heightened ML/TF risk according to the subject of

assessment's risk assessment methodology;

f) the geographical area of the business activities, in particular where they are carried out in high-risk third countries,[18]as well as, if applicable, the countries of origin or establishment of a significant part of the subject of assessment's customers and the geographical links of its qualifying shareholders or beneficial owners;

g) the authorisations, licensing or passporting by the subject of assessment.

45. In order to develop a good understanding of residual risk factors to which subjects of assessment are exposed, competent authorities should gather information from different sources that includes, but is not limited to, the information in respect of:

a) the adequacy of mitigating measures put in place by a subject of assessment and in particular information

i) relating to the adequacy of the risk-management framework, including the ML/TF risk management;

ii) from the internal controls function reports, including internal audit, where relevant;

iii) related to the prudential and general aspects of the subject of assessment's business, such as years in operation, liquidity or capital adequacy;

iv) findings from off-site reviews carried out by the competent authority, other relevant competent authority, prudential supervisors or other relevant supervisory authority, including AML/CFT authorities in third countries.

b) the effectiveness of mitigating measures put in place by a subject of assessment, in particular information in respect of:

i) the quality of internal governance arrangements and structures, including the adequacy and effectiveness of internal audit and compliance functions, reporting lines, the level of compliance with AML/CFT legal and regulatory requirements and the effectiveness of the AML/CFT policies and procedures to the extent that these are already known;

ii) the prevailing 'corporate culture', particularly the 'compliance culture' and the culture of transparency and trust in relations with the competent authorities;

iii) findings from previous supervisory inspections carried out by the competent authority, other relevant competent authority, prudential supervisors or other relevant supervisory authority, including AML/CFT authorities in third countries that involve certain on-site elements and testing;

iv) pending or imposed supervisory measures and sanctions related to the subject of assessment taken by the competent authority, prudential supervisors or other relevant supervisory authority, including in third countries;

[18] 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.

v) Information received from financial intelligence units, such as the information related to suspicious transactions reports.

46. Where competent authorities consider that the information gathered through sources described in paragraphs 30 and 31 is not available or is insufficient to develop a good understanding of risks associated with the subject of assessment, competent authorities should consider collecting such information directly from the subjects of assessment.

47. Where information for the individual risk assessment is gathered directly from subjects of assessment, competent authorities should ensure that the type of information requested is determined by the relevant domestic, foreign and sector-wide risk factors as set out in these guidelines, including emerging risks.

48. Competent authorities should consider adjusting the level and frequency of information requested from subjects of assessment based on the risk level associated with the sector or subsector to which the subject of assessment belongs. This means that information related to the sectors that are exposed to more significant levels of ML/TF risks may be collected more frequently than sectors with less significant levels of risk. When determining the level and frequency of the information requests, competent authorities should consider:

a) whether some of the information requested is available to the competent authority from other sources, including prudential supervisors, to reduce the duplication of information requests;

b) the purpose for which the information will be used. If the information is requested to inform the competent authority's assessment of risks associated with a subject of assessment or the sector, then the competent authority should consider aligning the frequency of information requests with the frequency of updates to the risk assessment;

c) whether there have been any significant changes to the level of ML/TF risk associated with the subject of assessment or the sector, which would indicate the need for more frequent information requests.

4.3 Step 2 – Risk assessment

4.3.1 General considerations

49. Competent authorities should take a holistic view of the ML/TF risk factors they have identified under Step 1 that, together, will form the basis for the individual risk assessments of subjects of assessment and the sectoral risk assessments.

50. When drawing up their risk assessment methodology, competent authorities should consider how sectoral and individual risk assessments interact. The sectoral risk assessment provides competent authorities with an overall view of the ML/TF risks to which subjects of assessment in a particular sector are exposed, and the relevance of individual risk factors to subjects of assessment in this sector. Through individual risk assessments, competent authorities should be able to assess the impact of sectoral risks on each subject of assessment, while at the same

time using those risk assessments to update and review their sectoral risk assessments as appropriate, including by identifying new risk factors that are common to subjects of assessment in the sector.

4.3.2 Sectoral and subsectoral risk assessment

51. Competent authorities should develop a good understanding ML/TF risks present in each sector under their supervision, which will allow them to prioritise their supervisory activities across and within sectors and to identify ML/TF risks that are relevant for a particular sector. The sectoral risk assessment should provide competent authorities with the basis for the individual risk assessment of subjects of assessment in that particular sector, by developing their understanding of the inherent risks within the sector to which subjects of assessment are exposed to inform the competent authority's understanding of the extent of supervisory attention needed in the sector. Competent authorities should decide whether they have sufficient, reliable information on controls within the sector to carry out the assessment of residual risk. Should this information be deemed insufficient, competent authorities should consider using the relevant supervisory tools at their disposal to obtain sufficient information, as set out in Section 4.4.4.

52. Competent authorities should ensure that the sectoral risk assessment is sufficiently comprehensive and enables the supervisor to obtain a holistic view of all relevant risk factors, and the extent to which they affect subjects of assessment in each sector.

53. In order to perform the sectoral risk assessment, competent authorities should first define the sectors and subsectors, where relevant, under their supervision as described in paragraphs 38 and 39 above.

54. When carrying out the risk assessment of the sector as a whole or of the subsector, if relevant, competent authorities should perform an assessment of the sector-wide risk factors identified in line with Step 1 of the RBS Model. Competent authorities should base their assessment on the information gathered in line with Section 4.2.6.

55. As part of this process, competent authorities should consider allocating different weights to different risk factors as described in paragraphs 63 and 64 of these guidelines, to reflect the degree of impact that various ML/TF threats have on the particular sector.

4.3.3 Individual risk assessments

56. Competent authorities should develop a comprehensive understanding of the inherent risks and, to the extent that they have access to sufficiently reliable data on the quality of the subject of assessment's AML/CFT controls, residual risks to which subjects of assessment are exposed. To that end, they should carry out individual risk assessments of each subject of assessment. Competent authorities should use all relevant sources to gather the necessary information for the individual risk assessments as described in paragraphs 44 to 48 above.

57. In order to achieve a comprehensive understanding of risks associated with individual subjects of assessment, competent authorities should establish and maintain an ongoing process and methodology for assessing and reviewing risks associated with the subjects of assessment. When developing their risk assessment processes, competent authorities should:

    a) Be guided by the outcome of the assessment of risks within the sector or subsector to which the subject of assessment belongs. In essence, with the sectoral or subsectoral risk assessment, the competent authority will have already identified the main inherent risks to which individual subjects of assessment within a given sector or subsector are exposed.

    b) Determine how they will assess the relevant inherent risk factors identified under Step 1 of the RBS Model that affect the subject of assessment.

    c) Gather the necessary information that allows them to understand the subject of assessment's exposure to customer, products and services, geographical and distribution channel risks. This means that competent authorities should consider whether the same information is required in respect of all subjects of assessment. Where information is gathered from the subjects of assessment, competent authorities should refer to the section on the 'Quality Assurance' in these guidelines for additional safeguards that should be put in place.

58. Where, on the basis of information set out in paragraph 45 b) in these guidelines, competent authorities have developed a sufficient and sufficiently reliable understanding of mitigating measures put in place by subjects of assessment, they should carry out the assessment of the residual risk in respect of those subjects of assessment. However, where such information is not available or reliable, or insufficiently comprehensive, competent authorities should use the inherent risk assessment in respect of those subjects of assessment instead.

59. When assessing the residual risk factors, competent authorities should take the steps necessary to assess the extent to which the AML/CFT systems and controls, which the subject of assessment has in place, are adequate to effectively mitigate the inherent risks to which it is exposed. As part of this, competent authorities should assess at least:

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

    b) that wider governance arrangements and risk-management processes, including overall risk culture, are adequate and effective.

60. Competent authorities should determine how to incorporate their professional judgment in their risk assessment work. Section 4.4.4. provides in that respect that the AML/CFT supervisory manual should allow competent authorities to ensure the application of the supervisory tools and professional judgment in a consistent way.

4.3.4 Assessment of the ML/TF risks at the group level

61. Competent authorities, who are the lead supervisor in accordance with the ESAs Joint Guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849[19], should develop a holistic view of ML/TF risks to which subjects of assessment which are part of a group are exposed. This means that these competent authorities should develop a risk profile of the subject of assessment under their supervision, taking into account all relevant domestic and foreign risk factors. They should pay particular attention to the risks associated with a subject of assessment's cross-border operations and the business activities of parts of their group in other jurisdictions, which may have a bearing on the overall risk profile of the subject of assessment. In particular, the risk assessment should reflect at least the risks arising from the subject of assessment's exposure to countries:

    a) that have been identified by the European Commission's as having strategic deficiencies in their AML/CFT regime, in line with Article 9(2) of Directive (EU) 2015/849;

    b) where the law prohibits the implementation of group-wide policies and procedures and in particular if there are situations in which the Commission Delegated Regulation (EU) 2019/758 should be applied;

    c) which, in accordance with credible and reliable sources[20], are exposed to high levels of corruption or other predicate offences to ML;

    d) countries or territories where terrorist organisations are known to be operating or that have been subject to economic financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union; and

    e) where, according to information from more than one credible and reliable source, serious concerns have been raised about the effectiveness and quality of the jurisdiction's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight. In this case, credible and reliable sources may include mutual evaluation reports by the Financial Action Task Force (FATF) or FATF-style Regional Bodies (FSRBs), the FATF's list of high-risk and non-cooperative jurisdictions, International Monetary Fund (IMF) assessments and Financial Sector Assessment Programme (FSAP) reports.

62. To inform the risk assessment of subjects of assessment which are part of a group, competent authorities, which are the lead supervisor, should cooperate and exchange relevant information with other competent authorities that are responsible for the AML/CFT supervision of parts of the group. For cross-border groups, if there is an AML/CFT college, the lead supervisor should make use of the information exchanged in the college to gather the necessary

[19] (JC 2019 81).

[20] According to EBA Guidelines under Article 17 and 18(4) of Directive (EU) 2015/849, the credibility of allegations can be determined on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations.

information for the risk assessment. Necessary information includes, in respect of branches or subsidiaries of subjects of assessment's, at least information related to:

a) the ML/TF risk profile of branches or subsidiaries as assessed by relevant competent authorities in those jurisdictions;

b) the ML/TF risk profile of the sector that has branches or subsidiaries as assessed by the relevant authorities in those jurisdictions,

c) findings from competent authorities' assessments of the quality of controls in place within branches or subsidiaries of subjects of assessment;

d) serious breaches or material weaknesses in branches or subsidiaries identified by relevant competent authorities in their jurisdictions;

e) any supervisory measures and sanctions imposed on branches or subsidiaries by relevant competent authorities in their jurisdictions.

63. When assessing whether subjects of assessment have implemented group-wide policies and procedures in their branches and subsidiaries effectively, competent authorities, which are the lead supervisor, should refer to the risk assessment in respect of these subjects of assessment described in paragraphs 57 and 58 of these guidelines and, in particular, the assessment of geographical risks to which branches and subsidiaries of subjects of assessment are exposed.

4.3.5 Weighting risk factors

64. Competent authorities should weight the risk factors for sectors and subjects of assessment identified under Step 1 of the RBS Model, depending on their relative importance. In this regard, there are a number of considerations that competent authorities should take the following into account:

a) When weighting inherent risk factors, competent authorities should make an informed judgement about the relevance of different factors in relation to a sector, subsector or individual subject of assessment. In respect of individual subjects of assessment, competent authorities should take into account their sectoral or subsectoral risk assessment.

b) The weight given to individual risk factors can vary between sectors, subsectors or subjects of assessment, but competent authorities should use similar factors for similar sectors, subsectors or subjects of assessment.

c) Weighting of risks does not lead to a situation where it is impossible for a sector, subsector or subject of assessment to be classified as a significant or very significant risk or where all sectors, subsectors or subjects of assessment fall within the same risk category.

d) Weighting is not unduly influenced by just one risk factor and that due consideration is given to factors that are identified by Directive (EU) 2015/849 or national legislation as always presenting a significant or high ML/TF risk. When weighting risk factors,

competent authorities should ensure that one risk factor does not sway the balance of the overall weighting to a disproportionate and unreasonable assessment.

65. Where competent authorities use automated IT systems to allocate overall risk scores to subjects of assessment, and in particular in situations where they have not developed these in house but purchased them from an external provider or otherwise relied on external input, they should understand how the system works and how it combines or weighs risk factors to achieve an overall risk score. Competent authorities should always be satisfied that the scores allocated reflect their understanding of ML/TF risk associated with the subject of assessment.

4.3.6 Risk profiles and categories

66. The assessment of the inherent risk level and the effect on the inherent risk level by risk mitigants should result in the assignment of a risk score, where relevant, to the sector, subsector and subject of assessment to facilitate comparison between subjects of assessment and to inform the action they take in Step 3.

67. Competent authorities should ensure that the assessment of mitigants within the subject of assessment, sector or subsector is based on reliable information, such as the information set out in point b) of paragraph 45 above. In the absence of such information, competent authorities should consider whether the inclusion of mitigating factors is justified, and whether, as a result of the allocation of scores to mitigating factors, the final ML/TF risk score of the subject of assessment is not distorted.

68. Where competent authorities have only limited or unverified information available to them about mitigants within the subject of assessment or sector and subsector, they should categorise these subjects of assessment, sectors and subsectors on the basis of their inherent risk profile and assign the residual risk score when relevant information becomes available.

69. Competent authorities should use their professional judgement to validate the results of the overall risk assessment of the subject of assessment or sector/subsector and correct it if necessary.

70. Competent authorities should decide on the most appropriate way to categorise the risk profiles of subjects of assessment, sectors and subsectors. To achieve convergence and facilitate cooperation and information exchange between different competent authorities, competent authorities should consider classifying subjects of assessment, sectors and subsectors as ‘very significant’, ‘significant’, ‘moderately significant’ and ‘less significant’ in line with the EBA’s ML/TF risk assessment processes.

71. Competent authorities should ensure that their risk assessment processes enable them to distinguish between inherent and residual risks. When categorising the inherent risk associated with subjects of assessment, sectors or subsectors, competent authorities should consider the following risk categories:

    a) less significant risk, where the subject of assessment, sector or subsector is very unlikely

to be abused extensively for ML/TF purposes;

b) moderately significant risk, where the subject of assessment, sector or subsector is unlikely to be abused extensively for ML/TF purposes;

c) significant risk, where the subject of assessment, sector or subsector is likely to be abused extensively for ML/TF purposes; or

d) very significant risk, where the subject of assessment, sector or subsector is very likely to be abused extensively for ML/TF purposes.

72. When categorising the residual risk associated with subjects of assessment, sectors or subsectors, competent authorities should consider the impact that mitigating measures may have on the inherent risk associated with subjects of assessment, sectors and subsectors. The four risk categories should be applied by competent authorities to categorise residual risk as follows:

a) less significant risk, where the inherent risk is less significant and the risk profile remains unaffected by mitigation, or where the inherent risk is moderately significant or significant, but is effectively mitigated through AML/CFT systems and controls;

b) moderately significant risk, where the inherent risk is moderately significant and the risk profile remains unaffected by mitigation, or where the inherent risk is significant or very significant, but is effectively mitigated through AML/CFT systems and controls;

c) significant risk, where the inherent risk exposure is significant and the risk profile remains unaffected by mitigation, or where the inherent risk is very significant but is effectively mitigated through AML/CFT systems and controls; or

d) very significant risk, where the inherent risk is very significant and, regardless of the mitigation, the risk profile remains unaffected by mitigation, or where the inherent risk is very significant and is not effectively mitigated due to systemic AML/CFT systems and control weaknesses in the subject of assessment or in the majority of subjects of assessment in the sector.

73. Where competent authorities decide not to apply the risk classification set out in paragraphs 69, 70 and 71 above, they should be able to convert their risk categories in line with those recommended in these guidelines. Competent authorities should adopt a conservative approach when converting the risk categories as described in the annex to these guidelines.

74. Competent authorities should note that the categorisation of subjects of assessment for ML/TF risk purposes may be different from categories applied to the same subjects of assessment for wider conduct risk or prudential risk purposes.

75. Where a competent authority uses an automated IT system to determine the risk profile or score of an individual subject of assessment, competent authorities should make allowances for situations where they may need to amend the results of the automated scoring on the basis of their professional judgment in addition to the review process set out in Step 4 of the RBS

Model. Competent authorities may decide to apply their professional judgment if there is information that suggests that the overall risk rating is not a true reflection of reality, including information from financial intelligence units, media reports, other supervisors or on-site and off-site supervision. The rationale for such changes to the risk profile or score should be clearly documented by the competent authority.

4.4 Step 3 – Supervision

4.4.1 General provisions

76. Competent authorities should ensure that subjects of assessment exposed to significant and very significant ML/TF risks are subject to more frequent and intrusive supervision than those exposed to moderately or less significant risks. Competent authorities should adjust their supervisory approach by adjusting one or more of the following elements:

    a) the nature of supervision, by adjusting the ratio between off-site and on-site supervisory tools;

    b) the focus of supervision, by focusing on the overall AML/CFT framework in place at subjects of assessment or by focusing on the management of specific ML/TF risks, including risks associated with particular products or services, or on specific aspects of the AML/CFT processes such as customer identification, risk assessment, ongoing monitoring and reporting activities;

    c) the frequency of supervision, by ensuring that subjects of assessment that are exposed to more significant ML/TF risks are supervised more frequently than those subjects of assessment that are exposed to less significant risks; and

    d) the intensity and intrusiveness of supervision, by determining, according to risk, the extent of customer file reviews, sample testing of transactions and suspicious transactions reports conducted on-site. Competent authorities should note that a review based only on an assessment of policies and procedures, rather than on their implementation, is unlikely to be sufficient in situations where the exposure to ML/TF risk is more significant.

4.4.2 Supervisory strategy

77. Competent authorities should determine and implement a longer-term AML/CFT supervisory strategy where they set out how they will mitigate the ML/TF risks they have identified in all sectors and subsectors, where relevant, under their supervision. The strategy should be based on the sector-wide risk assessment carried out by competent authorities in accordance with Guideline 4.3.

78. 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 and with available resources. As part of this, a supervisory strategy should:

    a) explain how they will work to mitigate the existing ML/TF risks identified in the sectors and

subsectors under their supervision;

b) explain how they will ensure that adequate supervisory coverage and monitoring commensurate with the ML/TF risk is applied to all sectors and subsectors, including those associated with lower ML/TF risks. In particular, how they will ensure that sectors associated with more significant ML/TF risks will receive higher supervisory coverage;

c) set out the type of supervisory tools that competent authorities will use to tackle which types of risks as described in Section 4.4.4. of these Guidelines;

d) define cycles of supervisory inspections and reviews, if any, according to which subjects of assessment in each risk category will be supervised and determine the type of supervisory tools applicable in each cycle;

e) determine the supervisory resources necessary to implement the supervisory strategy and ensure that sufficient resources are available to them;

f) 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.

4.4.3 AML/CFT supervisory plan

79. Competent authorities should determine and put in place a supervisory plan for all subjects of assessment, which explains how their supervisory strategy will be implemented in practice. Competent authorities should decide on the period of time covered by their supervisory plan, such as an annual or two-yearly supervisory plan, taking into account wider organisational constraints as appropriate.

80. Competent authorities should coordinate all supervisory plans that cover the entire time period covered by the supervisory strategy to ensure balance between them and that together they serve to implement the supervisory strategy. This means that where the supervisory strategy is set for a 5-year period but the supervisory plans are developed annually, competent authorities should ensure that all annual plans together over the 5-year period fulfil the strategy.

81. In the supervisory plan, competent authorities should clearly set out the supervisory tools that they will apply to subjects of assessment to achieve their objectives in line with their strategy. Competent authorities should use risk assessments of individual subjects of assessment to fine-tune their choice of supervisory tools for a specific subject of assessment targeting risks specific to that subject of assessment.

82. Competent authorities should set out in the plan how they will allocate supervisory resources to subjects of assessment in a way that is commensurate with the subjects of assessment's risk profile developed in line with Guideline 4.3.

83. Competent authorities should recognise that subjects of assessment exposed to significant or very significant levels of ML/TF risk may not be systemically important. Therefore, when deciding on the most appropriate AML/CFT supervisory tools, competent authorities should

refer to their ML/TF risk assessment and should not rely on their prudential or conduct risk assessments, where available, nor should they consider only systemically important subjects of assessment. Competent authorities should note that it may not be appropriate to draw conclusions for AML/CFT supervisory purposes from the level of prudential or conduct risk.

84. Competent authorities should ensure that the AML/CFT supervisory plan is independent from the prudential supervisory plan; although, at times, there might be overlaps in the subjects of assessment inspected by competent authorities and prudential supervisors, and joint or supplementary supervisory tools may be applied. However, competent authorities are responsible for ensuring that the AML/CFT supervisory objectives are fully met as a result of these actions.

85. When developing the AML/CFT supervisory plan, competent authorities should ensure that they provide for contingencies in cases where new risks are identified in the course of on-site or off-site supervision or through other reliable sources, which require competent authorities to respond in an appropriate and timely fashion.

86. Where competent authorities are required to make amendments to the initial AML/CFT supervisory plan, such as changing from off-site to on-site supervision or from thematic reviews to full scope inspections, to adapt to the new circumstance or to tackle the emerging ML/TF risks, they should have appropriate internal governance arrangements in place when processing such changes to the supervisory plan. All such changes should be adequately documented by competent authorities, explaining how and when the supervision of those subjects of assessment affected by changes to the plan will be carried out.

4.4.4 Supervisory tools

87. Competent authorities should recognise that each subject of assessment, sector and subsector is exposed to different levels of ML/TF risk and, therefore, the type and frequency of supervisory tools used may differ between them. To ensure efficient use of supervisory resources, competent authorities should choose such supervisory tools likely to have a greater impact on the subjects of assessment's compliance, or allow them to cover a larger part of a sector. Where competent authorities are looking to develop a better understanding of the way specific ML/TF risks are managed by a sector, or particular types of subjects of assessment, they should consider using thematic reviews to achieve this.

88. Competent authorities should have a good understanding of all supervisory tools available to them to implement their supervisory strategy and plan. They should develop an understanding of the advantages and disadvantages associated with each supervisory tool, including the level of intrusiveness and intensity they could achieve with each of the supervisory tools, and consider how they can use the widest range of supervisory tools at their disposal effectively, including, but not limited to, full scope or partial on-site inspections, ad hoc inspections, thematic inspections, AML/CFT returns, follow-up inspections, off-site reviews, as well as the feedback and guidance to the sector.

89. Competent authorities should select the most effective supervisory tools for subjects of assessment to address a specific supervisory need or objective. When selecting supervisory tools, competent authorities should refer to their sectoral and individual ML/TF risk assessments and should also consider:

    a) the number of subjects of assessment and sectors under the competent authority's supervision;

    b) specific features of different supervisory tools when applied on their own or in combination with each other;

    c) the resources needed to apply different supervisory tools;

    d) the time needed for the supervisory tool to achieve its purpose and to have an impact on the subjects of assessment's AML/CFT compliance.

90. Competent authorities should exercise flexibility to be able to adapt their use of supervisory tools also in response to emerging ML/TF risks within the subject of assessment, sector or subsector as they arise. This means that where competent authorities have identified an emerging ML/TF risk, either through AML/CFT returns, other supervisory tools or other means, they should consider whether a further and more intrusive assessment through an off-site review or an on-site inspection may be necessary to ensure that the subjects of assessment's systems and controls are sufficiently robust to mitigate the emerging risk. Therefore, on-site inspections allow competent authorities to:

    a) develop a deeper understanding of the subject of assessment's overall approach towards AML/CFT, including practices, governance, staff behaviours and culture;

    b) discuss potential risks, the results of supervisory activities, as well as problems which the subject of assessment might be facing and ways to solve them;

    c) communicate their supervisory expectations directly to subjects of assessment.

91. Either on their own or in combination with other supervisory tools, competent authorities should consider using on-site inspections, in particular, when supervising subjects of assessment that present a significant and very significant level of ML/TF risk. These inspections include, at least, a review of subjects of assessment's AML/CFT policies and procedures and an assessment of how they are implemented in practice through, inter alia, interviews with key personnel, testing of systems used in the AML/ CFT compliance and a review of the risk assessment and customer files. Based on the scope and complexity of the subjects of assessment's business, competent authorities should consider whether the full scope on-site inspection will cover the entire business of the subject of assessment or whether it is more feasible to focus on a specific business line within the subject of assessment. Although, where the scope is limited to a specific business line, competent authorities should develop an understanding of the touch points between the systems and controls applied within that business line and those applied in the wider institution and, where weaknesses in the business line's systems and controls are identified, competent authorities should seek to assess whether and how this may have an impact on the entire subject of assessment.

92. When deciding whether to carry out a full-scope on-site inspection at the subject of assessment, competent authorities should consider the following factors:

    a) whether there is a need to obtain additional or more comprehensive information on the subject of assessment that may be obtained only through on-site elements;

    b) what type of information is needed and how to obtain it effectively and in a comprehensive manner;

    c) whether the outcomes of previous on-site inspections or off-site reviews carried out either by the competent authority or relevant prudential supervisors or, where the subject of assessment is part of a group, by competent authorities responsible for the supervision of other entities within the group, if available, show poor levels of AML/CFT compliance or suggest poor compliance culture within the subject of assessment or within the group, which may have an impact on the subject of assessment;

    d) whether subjects of assessment have previously breached their AML/CFT obligations and whether they have done so repeatedly;

    e) what type of supervisory follow-up, if any, was previously applied by the competent authority to the subject of assessment; and

    f) whether subjects of assessment have previously demonstrated their commitment to fix the shortcomings and whether they have taken robust action to do so.

93. Competent authorities should consider using off-site reviews in those instances where a less intrusive supervisory approach might be sufficient, or in cases where subjects of assessment are exposed to low levels of ML/TF risk. Off-site reviews primarily involve a desk-based review of the subjects of assessment's written AML/CFT policies and procedures and the risk assessment, but does not involve an in-depth assessment of how effectively these policies and procedures have been implemented in practice by the subject of assessment. Off-site reviews may also be considered as a preliminary step to more thorough reviews through on-site inspections that would complement off-site work, or may be used in combination with other supervisory tools.

94. 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, significant changes in the ML/TF risk exposure of the sector/ subsector or subjects of assessment or happen as a result of discovery of certain information by the competent authority, including through whistleblowing reports,

widespread public allegations of wrongdoing, 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.

95. Where competent authorities undertake an inspection remotely through virtual means, they should consider the effectiveness of this supervisory tool and whether the engagement with the subject of assessment meets the conditions for an on-site inspection and is commensurate with the ML/TF risk presented by the subject of assessment. Competent authorities should consider whether an on-site inspection is more appropriate when supervising subjects of assessment that present a significant or very significant level of ML/TF risk and in circumstances where competent authorities are looking to develop a deep understanding of the overall AML/CFT systems and controls framework within the subject of assessment.

96. Competent authorities should consider the most effective supervisory tool to ensure that group-wide policies and procedures are implemented effectively by subjects of assessment, which are part of the group by applying similar considerations to those applicable to individual subjects of assessment as explained above. If a group is operating on a cross-border basis, the lead supervisor [21] should cooperate with other competent authorities involved in the supervision of subjects of assessment within the group through AML/CFT colleges, where they exist, or through other channels and cooperation mechanisms, including those set out in the EBA's Cooperation Guidelines.[22] This cooperation may consist of, but is not limited to:

a) the extent of mutual assistance described in Guideline 9 of the AML/CFT Colleges Guidelines;

b) agreeing to apply a particular supervisory tool or supervisory action with other competent authorities, which are responsible for the supervision of other subjects of assessment within the group. This may involve carrying out an inspection or a review jointly with other competent authorities or by jointly adjusting the focus of a supervisory tool to mitigate risks that are cross-cutting across the group more effectively;

c) exchanging information relating to the ML/TF risk assessment of the subject of assessment or the sector, if relevant;

d) exchanging information related to planned supervisory inspections or reviews and on relevant findings thereafter;

e) exchanging information related to weaknesses or breaches identified by other competent authorities.

[21] The lead supervisor is determined in accordance with the ESAs joint guidelines (JC 2019 81) on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions ('the AML/CFT Colleges Guidelines'). In general, the lead supervisor is a competent authority that is responsible for the AML/CFT supervision in a Member State where the head office of the group is located.

[22] EBA Guidelines on Cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Article 117(6) of Directive 2013/36/EU, December 2021

97. Competent authorities should have a holistic view of all supervisory tools applied by them. They should monitor their implementation and effectiveness and make adjustments where necessary.

4.4.5 Supervisory practices and the supervisory manual

98. To meet their obligations under Directive (EU) 2015/849, competent authorities should ensure that subjects of assessment have put in place robust AML/CFT systems and controls and that these systems and controls are sufficiently effective to prevent and detect ML/TF. The steps competent authorities take to assess subject of assessments' AML/CFT systems and controls should be set out in a dedicated AML/CFT supervisory manual. This allows competent authorities to ensure the application of the supervisory tools and professional judgment in a consistent way. When drafting the manual, competent authorities should ensure that it provides sufficient details of all the activities relevant supervisors are required to undertake to carry out supervision effectively, however it should also provide supervisors with sufficient flexibility to apply their expert judgement and make adjustments to the supervisory approach as necessary.

99. Competent authorities should ensure that, where relevant, subjects of assessment appoint AML/CFT compliance officers in accordance with Article 8(4) of Directive (EU) 2015/849. Competent authorities should also take risk-sensitive steps to check whether the AML/CFT compliance officer appointed by a subject of assessment has or continues to have the necessary levels of integrity, expertise and knowledge to fulfil its functions effectively.[23] This may include a meeting with the AML/CFT compliance officer or requesting the subject of assessment to provide a summary of the AML/CFT compliance officer's professional expertise and any other information deemed relevant by the competent authority. Competent authorities should consider whether to carry out such an assessment as part of their supervisory activities, including during on-site inspections or off-site reviews, or as a stand-alone assessment.

100. Where, as a result of checks described in paragraph 99, the competent authority is concerned that the AML/CFT compliance officer may not be suitable, the competent authority should notify the relevant prudential supervisor[24] of their concerns and should proactively share with prudential supervisors any information that has given rise to these concerns. Furthermore,

    a) where the assessment of the suitability of the AML/CFT compliance officer is not within the competence of a prudential supervisor, competent authorities should apply the necessary measures to remedy the issue without undue delay, such as a request for the AML/CFT compliance officer to undergo additional training or an enhancement of professional qualifications; a request for an enhanced management or the reorganisation of the

[23] Consultation Paper on Draft 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.

[24] In accordance, in particular, with paragraph 19 of the forthcoming EBA Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU

AML/CFT compliance officer's role; or a request for the replacement or an additional AML/CFT compliance officer to be appointed;

b) where prudential supervisors are competent for assessing the suitability of the AML/CFT compliance officer,[25] competent authorities should cooperate with prudential supervisors during the initial assessment and also during any reassessments of suitability by prudential supervisors as necessary.[26] Competent authorities should share all relevant information, which may have an impact on the suitability assessment or reassessment of the AML/CFT compliance officer, with relevant prudential supervisors, including their proposed recommendations of measures, as described in point a) above, that could be taken from an AML/CFT supervisory perspective to mitigate the issues.

101. In the supervisory manual, competent authorities should outline the steps supervisors are required to take when applying different supervisory tools. The manual should set out at least:

a) the process and methodology followed by competent authorities when assessing ML/TF risks associated with subjects of assessment and sectors/subsectors. Competent authorities should also explain the process followed by supervisors when they wish to amend the risk score of the subject of assessment based on their professional judgment;

b) possible instances where supervisors are required to cooperate with other stakeholders as described in Section 1.4.1 of these Guidelines and explain the process of how this cooperation should happen in practice;

c) the process that should be followed by supervisors when carrying out each supervisory tool and explaining the elements that should be tested. Competent authorities should clearly set out the key differences between different supervisory tools available to them. This means that competent authorities should at least clarify the extent to which supervisors are expected to test in subjects of assessment:

   i) the adequacy of relevant policies and procedures and whether they are linked to the business-wide risk assessment;

   ii) that relevant processes have been put in place and that they operate as expected;

   iii) the adequacy and completeness of the business-wide risk assessments and to what extent it determines the overall AML/CFT approach;

   iv) the adequacy of customer risk assessments and the extent to which they determine the applicable level of customer due diligence requirements;

   v) the adequacy of internal governance arrangements and internal reporting lines, in respect of AML/CFT compliance, including the quality and quantity of management information;

[25] 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.

[26] Including as envisaged in Sections 6.1 and 6.3 of the forthcoming EBA Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU

vi) the adequacy of the person performing the role of the AML/CFT compliance officer within the subject of assessment as defined in Article 8(4) of Directive (EU) 2015/849 and steps that supervisors should take to carry out this assessment;

d) what type of engagements and communications should the supervisor have with the subject of assessment prior to, during and after the application of a particular supervisory tool;

e) when communicating findings from inspections or reviews, indicative timeframes that should be observed by competent authorities and subjects of assessment;

f) how to assess that AML/CFT systems and controls put in place by subjects of assessment are effective enough and commensurate with the ML/TF risks to which the subject of assessment is exposed. Competent authorities should at least set out the main areas on which the supervisor should focus, which may suggest the lack of effectiveness within the subject of assessment. Some indicators that may suggest that the AML/CFT framework is implemented effectively include, but are not limited to:

vii) staff within the subject of assessment demonstrate good understanding of the parameters used for different systems and are able to explain the rationale for the outcomes from these systems;

viii) systems and processes used to screen customers and transactions deliver the expected outcomes, which are in line with other similar subjects of assessment in a sector;

ix) policies and processes to identify and analyse suspicious or unusual transactions and report to the FIU or other relevant authorities;

x) staff at the subject of assessment demonstrate good understanding of AML/CFT policies and processes and how they are applied in practice;

xi) various internal and external reports, such as internal and external audit or consultants, do not raise any concerns about the subject of assessment's AML/CFT compliance;

xii) sufficient and relevant training is provided to all relevant staff and senior management within the subject of assessment;

xiii) fair incentives practices, including remuneration and other rewards, have been implemented by the subject of assessment that do not directly or indirectly foster unsound work practices or culture;

xiv) sufficient and adequate management reporting throughout all levels of management;

xv) adequate governance arrangements have been put in place with a clear role of the senior management within the AML/CFT framework.

g) the extent to which the supervisor is expected to challenge the robustness of AML/CFT

systems and controls, the implementation of AML/CFT policies and procedures and the effectiveness of the business-wide risk assessment;

h) examples of the type of situations where the supervisors are expected to apply their supervisory judgment;

i) where a supervisory tool includes sampling of customer files or transactions, the manual should explain the sampling methodology, including the minimum sample size and criteria for selecting a sample;

j) the steps that supervisors are required to take following the inspection to ensure that supervisory findings are adequately addressed by subjects of assessment and examples of instances in which a follow-up inspection may be necessary as set out in Section 4.4.8 of these Guidelines; and

k) the governance arrangements within the competent authority for approval of the outcomes from inspections or reviews, including the decision-making process relating to sanctions and administrative measures.

101. A) When developing their sampling policy, competent authorities should be mindful that subjects of assessment differ in many ways, such as the number and type of products and services and the number and type of customers and transactions. This means that competent authorities may need to tailor their approach to sampling in relation to a particular subject of assessment. As part of this, competent authorities should consider at least the following criteria for selecting a meaningful sample:

a) Sampling should help competent authorities to meet the objectives of a particular supervisory tool which is being used for the assessment. This means that a sample should be made up of a meaningful number of customer files or transactions that represent the diversity of customers, products and services in different risk categories, however the size and composition of that sample is determined by:

i) the goal of the supervisory tool used for the assessment;

ii) different risk categories of customers within the subject of assessment and the proportion of customers that represent significant or very significant ML/TF risk;

iii) the nature, size and complexity of the subject of assessment's business.

b) Checks performed as part of sampling should be sufficiently comprehensive and intrusive to enable the competent authority to achieve the desired supervisory goal.

c) Sampling should be balanced against other supervisory activities that form part of the supervisory tool, such as reviewing systems, governance arrangements and policies and procedures.

102. Competent authorities' sampling policy should be flexible and allow for adjustments based on the level of risk or new information, including information obtained as part of their supervisory activities. This means that competent authorities may change the size of the sample, the

categories of customers, products, services or transactions included in the sample or the specific checks performed prior to or during the inspection or review. Where sampling suggests a systemic failure to comply with the applicable AML/CFT obligations on behalf of the subject of assessment, competent authorities should investigate the root cause of this failure, which may involve further checks or supervisory activities, including additional sampling or interviews with key personnel.

103. The supervisory manual should be reviewed regularly and updated when necessary, in particular, if there have been significant changes that may have an impact on the supervisory approach, including changes introduced by the legal framework or international guidance, or changes required as a result of the feedback received by competent authorities on the adequacy of its supervisory approach, including from an internal audit function or external bodies like the Financial Action Task Force, the Council of Europe or the European Supervisory Authorities. As a result of this review, competent authorities should take stock of lessons learnt and address any shortcomings identified, if any. Relevant supervisors should be made aware of any changes to the manual without delay.

4.4.6 Quality assurance

104. Competent authorities should ensure that AML/CFT supervision is carried out consistently by all supervisors. Therefore, they should put in place quality assurance checks to ensure the consistent application of supervisory tools and practices by all supervisors in line with the supervisory manual. Such checks should include, at least, a review by the internal audit function and an application of a four-eye principle. Competent authorities should also make use of staff training, mentoring and work shadowing between supervisors as other means of achieving supervisory consistency.

105. Competent authorities should ensure the accuracy and reliability of information gathered from subjects of assessment for the purposes of the risk assessment or other supervisory tools. To ensure this, competent authorities should at least cross-check this information against the information already available to them in respect of the specific subject of assessment or similar subjects of assessment or against the information received from other reliable sources, including prudential supervisors, other competent authorities or financial intelligence units.

106. Where competent authorities have identified that the information provided by one or more subjects of assessment appears to be inaccurate or incomplete, they should take steps to clarify these inconsistencies and seek to obtain accurate information. In such circumstances, competent authorities should consider the most adequate supervisory action to address the issue based on the extent and type of inaccuracies identified. The actions may include requesting clarifications directly from the subject of assessment, carrying out an ad hoc inspection on the subject of assessment or imposing certain supervisory measures.

107. Competent authorities should consider the resources required when designing and carrying out the necessary quality assurance checks. In some instances, it may be necessary to involve certain specialised resources from IT or other fields.

4.4.7 Use of services of external parties

108. Where competent authorities use services of external consultants or auditors to carry out their supervisory plan, some parts of the plan or a specific supervisory task, they should always ensure that these external parties:

a) have sufficient knowledge and skills to carry out the specific supervisory tasks for which they are engaged by competent authorities;

b) have a clear understanding of regulatory expectations and the scope of work they are required to carry out;

c) have access to specific guidance that clearly sets out the terms of their involvement, as well as any processes that they are required to follow as part of their engagement;

d) keep sufficient records detailing the steps they have taken to carry the required tasks and explaining the rationale for their conclusions and findings;

e) carry out the required tasks to a high-quality standard. This may involve competent authorities reviewing other work carried out by the external party or participating in some of the activities carried out by them on behalf of the competent authority;

f) declare any potential conflicts of interest and, if it transpires that conflicts of interest exist, competent authorities should ensure that they are adequately managed and resolved. Where it is not possible to resolve the conflicts of interest, competent authorities should refuse or terminate the engagement with the specific external party.

109. Where competent authorities use experts consistently as part of their supervisory process, they should reflect this in the supervisory plan and manual.

110. Competent authorities should ensure that they maintain sufficient in-house expertise to be able to review and sufficiently challenge, if necessary, the work carried out by external parties on their behalf.

111. In situations where external auditors or consultants are engaged by subjects of assessment to carry out an assessment of their compliance with AML/CFT obligations, either on their own initiative or upon request by competent authorities, competent authorities should ensure that they are:

a) notified of the scope of the review carried out by the external parties;

b) notified of the skills, knowledge and experience of experts employed by the external parties who will carry out the assessment; and

c) updated regularly on the outcomes and findings of the experts' work, including where the experts consistently report the absence of weaknesses or findings.

112. Competent authorities should consider the work of external parties, and should reflect on it in their supervisory follow-up or as part of their ongoing supervision as necessary. Competent

authorities should analyse the reasons for any discrepancies identified between the work of experts from external parties and their own findings from supervisory inspections or reviews and reflect this analysis in their risk assessment of the subject of assessment. If competent authorities have doubts about the overall quality of work carried out by experts from external parties as described in paragraphs 108 and 111, competent authorities should consider including a review of this work as part of their future inspections or reviews within the subject of assessment.

113. Competent authorities should ensure that there are gateways in place to ensure that experts from external parties are able to report any irregularities, weaknesses or breaches within the subject of assessment directly to competent authorities, if necessary, regardless of whether their services are engaged by competent authorities or by subjects of assessment.

4.4.8 Supervisory follow-up

114. Competent authorities should be confident that all breaches or weaknesses in subjects of assessment's AML/CFT systems and controls framework are adequately addressed and effectively remediated by subjects of assessment. Competent authorities should take all necessary steps to ensure that subjects of assessment's behaviours or activities change or discontinue.

115. When deciding on the most effective supervisory follow-up, competent authorities should choose supervisory tools or measures that are proportionate to the materiality of weaknesses and seriousness of breaches identified and take into consideration the level of risk to which the subject of assessment is exposed. This means that serious breaches and material weaknesses[27] identified in a subject of assessment, which is exposed to significant or very significant ML/TF risk, will require more intense follow-up and more supervisory resources than less serious breaches or non-material weaknesses in less significant risk subjects of assessment. For example, in the most serious cases, competent authorities may carry out a follow-up inspection to ensure that all weaknesses are mitigated effectively and potentially consider a sanction, whereas in less serious cases, it may be sufficient to receive the confirmation from the subject of assessment that issues have been addressed in accordance with the remediation plan proposed by them.

116. When determining the most effective supervisory follow-up in accordance with paragraphs 114 and 115 above, competent authorities should consider at least:

a) whether, after the implementation of the remediation plan proposed by a subject of assessment to the competent authority, all breaches and weaknesses will be addressed and remediated effectively. Competent authorities should be satisfied with the timeline proposed by the subject of assessment for when the remediation will be complete, and they should challenge the subject of assessment where the timeline is unrealistic or where the proposed actions are not sufficiently robust to remediate specific weaknesses;

[27] For more details on how to determine the materiality of weaknesses, refer to the Regulatory Technical Standards developed by the EBA under Article 9a of the EBA Regulation.

b) whether to use one or a combination of supervisory tools, supervisory measures or sanctions to ensure that breaches and shortcomings within the subject of assessment are addressed and remediated in a most effective and timely manner;

c) the urgency of remediation as some breaches or weaknesses may require more urgent action by subjects of assessment, which means that competent authorities should ensure that sufficient priority is given by the subject of assessment to remediate these shortcomings;

d) the length of time required to remediate specific breaches or shortcomings and where the remediation may take a long time, the subject of assessment should put in place adequate temporary measures to mitigate the risk;

e) the probability of a repeat or systemic breach or weakness, which may be assessed by looking at the previous failures within the subject of assessment and the length of time for which the subject of assessment failed to implement effective systems and controls, the competent authority's follow-up should focus not just on fixing one specific issue but on ensuring the discontinuation of the systemic failure by the subject of assessment;

f) potential impact of the breach or weakness on the wider internal controls framework within subjects of assessment, which may require an engagement with prudential supervisors in accordance with the EBA's Cooperation Guidelines[28] and a possible follow-up action also from a prudential perspective;

g) the subject of assessment's ability and willingness to remediate failures identified by competent authorities, including the extent to which the key function-holders and senior management within the subject of assessment are involved in the remediation process.

117. 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 and exchange information on the subject of assessment's failures with prudential supervisors.

118. Competent authorities should formalise their supervisory follow-up process and set it out in their supervisory manual, while allowing sufficient flexibility for the supervisory judgement. Competent authorities should establish a timeline and a description of the concrete supervisory follow-up actions and measures to be taken by the subject of assessment to address each breach or weakness.

119. Where competent authorities have identified that subjects of assessment have failed to implement their group-wide policies and procedures effectively in all parts of the group in accordance with Article 45(1) of Directive 2015/849 and that their systems and controls are not

[28] EBA Guidelines on Cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Article 117(6) of Directive 2013/36/EU, December 2021

sufficiently robust to mitigate the risk to which the group is exposed in different jurisdictions, the competent authority should take the necessary steps to ensure that:

a) subjects of assessment have put in place a remediation plan at a group level setting out how they will remediate the identified weaknesses in different jurisdictions;

b) they cooperate with other competent authorities involved in the supervision of the group entities without delay, either through AML/CFT colleges or through other cooperation mechanisms, to ensure that they are aware of these weakness; and

c) they cooperate with other competent authorities and, potentially, prudential supervisors to decide on the most appropriate follow-up action, either at a group or individual entity level, as necessary. Such follow-up may involve, among other supervisory tools, a joint on-site inspection or a common approach between different competent authorities.

120. While the supervisory follow-up process is separate from the sanctioning process, the two processes are not mutually exclusive and should supplement each other. Therefore, irrespective of the sanctions to be imposed on a subject of assessment, competent authorities should closely follow-up to ensure that breaches and shortcomings are sufficiently remediated.

121. Without regard to the provisions in these guidelines, competent authorities should report any material weaknesses to the European Banking Authority in accordance with the draft regulatory technical standards under Article 9a of Regulation (EU) No 1093/2010.

4.4.9 Feedback to the sector

a. Feedback on risk assessments

122. Competent authorities should provide feedback to subjects of assessment on the outcomes of their sectoral risk assessment. Competent authorities should disclose at least:

a) the key risks they have identified in each sector and sub-sector;

b) their assessment of these risks; and

c) any other information that may enhance subjects of assessment's understanding of risks and enhance their business-wide and individual risk assessments.

123. Where competent authorities decide to provide subjects of assessment with a redacted version of their sectoral or subsectoral risk assessment, they should ensure this contains sufficient and meaningful information to enable subjects of assessment to use this information when developing their own risk assessments.

b. Guidance to the sector

124. Competent authorities should issue the necessary guidance to subjects of assessment explaining how they expect subjects of assessment to implement the risk-based approach in practice and what they are expected to do to comply with their AML/CFT obligation. Competent

authorities should use relevant guidelines published by the European Supervisory Authorities as a basis for their guidance, supplementing them with specific features at a national level.

125. Competent authorities should also assess the need for further guidance in the sector. Competent authorities should assess the level of AML/CFT knowledge and expertise in their sector based on reoccurring issues, emerging risks or other concerns arising from their analysis of information gathered for the risk assessment, findings from inspections, including thematic reviews, and from other engagements with the sector, including trade associations. Some of the indicators that may suggest that further guidance may be needed, include but are not limited to:

a) repeated failures by subjects of assessment to comply with certain AML/CFT obligations;

b) recent changes in the legislative framework at the national or EU level that may have an impact on subjects of assessment's ability to comply with their AML/CFT obligations;

c) evidence of de-risking in some sectors or subjects of assessment, or evidence that subjects of assessment avoid risks rather than manage them effectively;

d) repeated questions addressed to competent authorities or requests for guidance on certain aspect of the AML/CFT framework;

e) emergence of new ML/TF risks and typologies.

126. Competent authorities should assess whether guidance may be needed for the sector as a whole or specifically for a particular subsector or cover a specific topic. Competent authorities should ensure that guidance provided by them is clear and unambiguous as well as:

a) facilitates and supports the implementation, by subjects of assessment, of an effective risk-based approach;

b) does not directly or indirectly foster or condone the indiscriminate de-risking of entire categories of customers in accordance with the EBA's ML/TF Risk Factor Guidelines and in particular Guidelines 4.9., 4.10. and 4.11.[29]

127. 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 trade associations, financial intelligence units, law enforcement, other competent authorities or government agencies or through 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.

[29] 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.

128. Competent authorities should periodically assess the adequacy of their existing guidance provided to the sector. Such 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, amendments to the national or supranational risk assessment or 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.

c. Communication with the sector

129. Competent authorities should put in place and apply a communication strategy to ensure that their communications with subjects of assessment remain focused on improving AML/CFT compliance in the sector or certain subsectors and to ensure the most effective use of competent authorities' resources. As part of their communication strategy, competent authorities should set out how they will communicate with different stakeholders, including when communicating the outcomes of their risk assessment and relevant guidance to the sector.

130. Competent authorities should identify the most adequate and effective communication tools available to them, which allow them to communicate their regulatory expectations to the relevant stakeholders in a clear and constructive manner. These tools may include, but are not limited to:

a) simultaneous communication with all subjects of assessment, which may include a publication on the competent authority's website or through other online channels;

b) communication to a limited group of stakeholders, which may include the competent authority's participation at various conferences or training events or through an outreach to trade and professional associations;

c) communication through letters or circulars, which may be addressed to the sector as a whole or relevant groups of stakeholders; or

d) direct communication with subjects of assessment either on a bilateral or multilateral basis, including public consultations. Where the competent authority communicates bilaterally, it should consider the relevance of this communication for a wider group of stakeholders, which may indicate that a potentially different communication tool may be more adequate.

131. When deciding on the most appropriate tools for communication, the competent authorities should consider at least the following elements:

a) the target audience of the communication, which may determine the granularity of the communication;

b) the relevance of a specific topic for a particular group of stakeholders, the sector or the market as a whole;

c) the timing and urgency of the communication, ensuring that the required information is made available to subjects of assessment in a timely manner; and

d) the type of information that is being communicated.

4.4.10 Training of competent authority's staff

132. Competent authorities should ensure that staff with direct or indirect AML/CFT responsibilities have appropriate knowledge and understanding of the applicable legal and regulatory AML/CFT framework and are suitably qualified and trained to exercise sound supervisory judgement.

133. Competent authorities should develop a training programme, which should be adjusted to meet the needs of specific functions within the competent authority, their job responsibilities, seniority and experience of staff. 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.

134. Competent authorities should ensure that their supervisory staff are trained in the practical application of the competent authorities' AML/CFT RBS Model so that supervisors are able to carry out risk-based AML/CFT supervision in an effective and consistent manner. Competent authorities should ensure that the outcomes of the sector-wide and individual ML/TF risk assessments are communicated to all relevant staff within the competent authority, including staff who are not directly involved in the risk-based AML/CFT supervision. Among other things, competent authorities should ensure that supervisors are able to:

a) understand the need for flexibility when subjects of assessment's views of risks and controls are different from competent authorities' views on those risks and take into consideration the argumentation provided by subjects of assessment;

b) assess the quality of the risk assessment carried out by subjects of assessment;

c) assess the adequacy, proportionality and effectiveness of subjects of assessment's AML/CFT policies and procedures and wider governance arrangements and internal controls in light of subjects of assessment's own risk assessment;

d) understand different products, services and financial instruments, and the risks to which they are exposed;

e) understand competent authorities' supervisory framework, including the AML/CFT supervisory strategy and plan; and

f) understand various supervisory tools used and practices put in place by competent authorities, and how they are relevant to the tasks carried out by the staff member, such as the use of different supervisory tools in practice, and the importance of cooperation with other stakeholders.

135. 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'. 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, other countries' AML/CFT supervisors.

136. Competent authorities should ensure that relevant training is provided in a timely manner especially for new staff and in case of significant changes within the AML/CFT supervisory framework. Competent authorities should ensure that the AML/CFT expertise of their staff remains up to date and relevant, and includes awareness of emerging risks, as appropriate.

4.5 Step 4 – Monitoring and updating of the RBS Model

4.5.1 Review of the risk assessment and supervisory strategy and plans (Steps 1, 2 and 3)

137. The RBS is not a one-off exercise, but an ongoing and cyclical process. Therefore, competent authorities should carry out periodic or ad hoc reviews of the information on which their risk assessment is based, and update this information as necessary.

138. As part of the cyclical process, competent authorities should review and update their sectoral and individual risk assessments of subjects of assessment regularly through periodic reviews or on an ad hoc basis.

139. Supervisory strategy and plans should also be updated as necessary, whether by establishing periodic reviews or as a response to external events. Supervisory strategy and plans should also reflect relevant changes to the risk assessments, in particular where emerging risks have been identified. Competent authorities should reflect the results of these reviews and updates as changes to the RBS.

a. Periodic reviews

140. Competent authorities should carry out periodic reviews of their individual and sectoral risk assessments to ensure that they remain up to date and relevant. As part of this, it is important that competent authorities verify that the underlying assumptions supporting the risk assessment are still up to date, including assumptions related to the different level of risks posed by the relevant sectors and subjects of assessment or the understanding of the effectiveness associated with a certain supervisory tool.

141. The schedule of each review should be aligned with the supervisory strategy and commensurate with the ML/TF risk associated with the sector and the subject of assessment. For sectors and subjects of assessment that are exposed to significant or very significant ML/TF risks or those facing frequent changes in their activities and operating in a fast changing environment, reviews should take place more frequently.

b. Ad hoc reviews

142. Ad hoc reviews of the risk factors, the risk assessment and, where necessary, the supervisory strategy and plans should take place following significant changes affecting the subject of assessment's risk profile, including:

a) emerging ML/TF risks;

b) findings from off-site and on-site supervision and any follow-up of corrective or remedial actions taken by the subject of assessment;

c) changes to, or new information emerging in relation to, owners of qualifying holdings, members of the management board or key function holders' operations or the organisation of the subject of assessment;

d) amendments to the European Commission's supranational risk assessment published in accordance with Article 6(1) of Directive (EU) 2015/849, national risk assessment or the supervisory risk assessment developed in line with these guidelines;

e) new types of firms entering the sector or subsector;

f) sudden changes within the sector or subsector, including changes to the customer base, services and products offered, delivery channels or exposure to certain geographic areas;

g) new information that has emerged suggesting that the ML/TF risk exposure in respect of a specific subject of assessment or sector has increased;

h) other situations where the competent authority has reasonable grounds to believe that information on which it had based its risk assessment is no longer relevant or has significant shortcomings.

143. Competent authorities should also consider whether changes affecting one particular subject of assessment might affect other subjects of assessment, and they should also review the risk assessment of those subjects of assessment, which are significantly affected by the change.

144. Where, as a result of the amended risk assessment the risk categories or scores have changed, competent authorities should ensure that their internal systems and supervisory manual are updated accordingly.

4.5.2 Review of the AML/CFT RBS Model

145. Competent authorities should seek to satisfy themselves that their internal processes and procedures, including their ML/TF risk assessment methodology, are up to date and are applied consistently and effectively. Competent authorities should review and update the methodology immediately, where necessary.

146. Where a review identifies issues with the AML/CFT RBS Model, competent authorities should take steps to address these. However, competent authorities should refrain from making repeated changes to their RBS Model within short time intervals, to facilitate comparisons over time.

147. Where competent authorities use automated scoring systems to carry out their risk

assessment, they should review the cases in which the automated score was amended based on a professional judgement, which suggested that the allocated score did not accurately reflect the subject of assessment's risk profile. In such cases, competent authorities should examine whether the extent and frequency of such amendments may not be an indication of an error in the risk assessment methodology. If an error is identified, competent authorities should take the necessary steps to rectify it.

a. Periodic reviews

148. Competent authorities should periodically review whether their AML/CFT RBS Model delivers the intended outcome and, in particular, whether the level of supervisory resources remains commensurate with the ML/TF risks identified. 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. These tools include, but are not limited to:

a) professional expertise;

b) self-assessment questionnaires;

c) sample testing of supervisory measures and actions;

d) new information such as reports and feedback from other competent authorities or relevant AML/CFT authorities,

e) feedback from financial intelligence units, law enforcement and other national agencies; or

f) publications by relevant European or international organisations.

149. Competent authorities should also seek to familiarise themselves with international best practices and consider participating in relevant international and European forums when possible.

150. Measuring the impact of AML/CFT supervision on the level of compliance and the effectiveness of subjects of assessments' AML/CFT controls may also help competent authorities assess the effectiveness of their AML/CFT RBS Model.

b. Ad hoc reviews

151. In addition to regular reviews at fixed intervals, competent authorities should review, update or amend their AML/CFT RBS Model if its adequacy or effectiveness is called into question by events such as:

a) External evaluations of the model, including by the FATF, Moneyval or external audits;

b) Internal evaluations of the model, including an internal gap analysis, internal audit reports, quality assurance testing and 'lessons learned' exercises;

c) Significant changes of the legislative or regulatory AML/CFT environment;

d) Publication of relevant international guidance; and

e) Emergence or identification of new risk factors.

4.5.3 Organisational and procedural aspects of the review process

152. Competent authorities should put in place an objective review process of their RBS Model, which is based on clear and transparent internal procedures. Such procedures should at least set out:

a) when the revision is due or what events would trigger the review;

b) what is the scope of the revision or how to determine the scope; and

c) who in the competent authority is in charge of the revision process. Competent authorities should consider whether the team or person within the competent authority who was responsible for setting up the RBS Model should also be responsible for the review of the model or whether a different person or team, such as the competent authority's internal quality assurance, internal audit or risk-management team should be responsible for the review.

153. In addition to the internal review process, competent authorities should consider whether it is necessary to engage an external expert to obtain an objective evaluation of its RBS Model or to ensure harmonisation on a national level with the models used by other competent authorities.

4.5.4 Record-keeping

154. Competent authorities should document the AML/CFT RBS Model, its implementation and subsequent reviews appropriately for its institutional (supervisory) memory and also to provide a record of outcomes and decisions and their underlying rationale to ensure that actions taken by competent authorities with regard to the different subjects of assessment are coherent and consistent.

4.5.5 Accountability

155. Senior management of the competent authorities should have an adequate understanding of the ML/TF risks present in the supervised sector and subsectors and be regularly informed on AML/CFT supervisory actions and their outcome. This is so they can judge the overall effectiveness of the measures implemented by the subjects of assessment to reduce these risks as well as the need to review, where appropriate, the intensity and frequency of the supervision and the allocation of supervisory resources.

156. Competent authorities' senior management should ensure that there are adequate governance arrangements put in place for approval of the supervisory strategy at a senior management level and any amendments thereafter and for monitoring the progress with the implementation of the AML/CFT supervisory strategy within the competent authority. In particular, they should ensure that the competent authority has sufficient resources to

implement the strategy, including AML/CFT specialist, legal, policy and risk-specialist resources, and that its supervisory objectives set out in the strategy are fully fulfilled.

Annex

Conversion of risk categories

Scenario 1: Where a competent authorities are categorising its subjects of assessment and sectors within three risk categories, they should apply the approach set out in Table 1 when asked to convert the risk categories into four categories as suggested by these guidelines.

Competent authority's risk categories	*Risk categories suggested in these guidelines*
Low risk →	Less significant risk
Medium risk →	Moderately significant risk
High risk →	Very significant risk

Scenario 2: : Where competent authorities are categorising their subjects of assessment and sectors in five risk categories, they should apply the approach set out in Table 2 when asked to convert the risk categories into four categories as suggested by these guidelines.

Competent authority's risk categories	*Risk categories suggested in these guidelines*
Low risk →	Less significant risk
Medium low risk →	Less significant risk
Medium high risk →	Moderately significant risk
High risk →	Significant risk
Ultra/very high risk →	Very significant risk

5. Accompanying documents

5.1 Cost-benefit analysis / impact assessment

A. Problem identification

1. Directive (EU) 2015/849, in line with international standards in combating money laundering and the financing of terrorism developed by FATF, puts the risk-based approach at the centre of the EU's AML/CFT regime. For firms, the risk-based approach is the basis of the application of a proper risk-management system. For competent authorities, risk-based approach serves to identify, understand and mitigate ML/TF risks and, based on the understanding of ML/TF risks to which sectors and firms are exposed, adjust resources accordingly in order to exercise a risk-based approach to AML/CFT supervision.

2. The legal basis for the application of a risk-based approach to AML/CFT supervision is set out in Article 48(6) of Directive (EU) 2015/849 , which requires competent authorities, when carrying out risk-based supervision to have a clear understanding of ML/TF risks in their jurisdiction, access to relevant information through both on-site and off-site supervisory activities and to adjust 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) 30 of Directive (EU) 2015/ 849 to issue guidelines containing the characteristics of a risk-based approach and the steps to conduct risk-based supervision. The EBA, together with EIOPA and ESMA, published these guidelines on 16 November 2016.

3. In addition, Directive (EU) 2018/843, was published on 19 June 2018 and had to be transposed by the Member States by 10 January 2020. Directive (EU) 2018/843 amended Directive (EU) 2015/849 and further strengthened the AML/CFT supervisory framework by including specific requirements for competent authorities to cooperate and exchange information between themselves and with other supervisors, including prudential supervisors and supervisors from third-country authorities. On this basis, the EBA, together with EIOPA and ESMA, published guidelines[31] that establish a framework and set out practical modalities for this cooperation to happen in AML/CFT supervisory colleges.

4. Directive (EU) 2019/2177 of 18 December 2019 amended Directive (EU) 2015/849 of 20 May 2015 and in particular Article 48(10) of Directive (EU) 2015/849. Thereafter, guidelines on the

[30] Article 48(10) of Directive (EU) 2015/849: By 26 June 2017, the ESAs shall issue guidelines addressed to competent authorities in accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 on the characteristics of a risk- based approach to supervision and the steps to be taken when conducting supervision on a risk-based basis. Specific account shall be taken of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down.

[31] Joint guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions (JC 2019 81).

characteristics of a risk-based approach to supervision and the steps to be taken when conducting supervision on a risk basis shall be issued in accordance with Article 16 of Regulation (EU) No 1093/2010 and shall be issued by the EBA from 1 January 2020.

B. Policy objectives

5. In the first version of the guidelines, the ESAs built on the high-level principles of risk-based supervision set out in Directive (EU) 2015/849 and explained the steps that supervisors should take to implement it in practice. However, the European Commission concluded in its post-mortem report of July 2019 that competent authorities found the application of the risk-based approach challenging in practice. The commission also concluded that the lack of cooperation between competent authorities had contributed to some of the issues raised in the report. In addition, mutual evaluations carried out by international bodies like the FATF and the IMF have also highlighted weaknesses in the supervisory approaches in a number of EU Member States. Moreover, the EBA's report on the competent authorities' approaches to AML/CFT supervision of banks published in February 2020 concluded that more detailed guidance may be needed in some areas of supervision to ensure that competent authorities are well equipped to identify and assess ML/TF risks to which firms under their supervision are exposed and that they take robust supervisory actions when they identify weaknesses in the firms' AML/CFT frameworks. Other EBA reports, such as the cum-ex report[32], pointed out that the guidelines need to strengthen the cooperation between AML/CFT supervisors and tax authorities.

6. To that end, the main objective of the revised guidelines is to develop further the concept of risk-based approach to AML/CFT supervision in order to achieve greater harmonisation of supervisory practices across the EU, while being mindful that competent authorities are at different maturity levels in the development of their supervisory approaches. To that end, the revised guidelines aim to clarify further what supervisors are required to do to identify and assess ML/TF risks associated with firms under their supervision by making a distinction between sector-wide and individual risk factors. To achieve this, the guidelines now elaborate further on the sources and type of information that supervisors need to obtain to carry out the risk assessment by placing specific emphasis on the information gathered through cooperation and the information gathered directly from the firms.

7. In addition, the guidelines provide additional guidance and explanations on how supervisors should use their risk assessment when developing their supervisory strategy and plans and how they should choose their supervisory tools to ensure they are commensurate with the risk to which the firm is exposed.

8. Regarding the greater harmonisation in the process of identifying and understanding ML/TF risks, the guidelines aim to introduce common ML/TF risk categories (i.e. less significance, moderately significant, significant and very significant). These proposed ML/TF risk categories are aligned with the methodology of the supranational risk assessment report published by the

[32] EBA Report on competent authorities' approaches to tackling market integrity risks associated with dividend arbitrage trading schemes (EBA/REP/2020/15).

Commission on July 2019 [33]. The amended guidelines also leverage recently developed regulatory instruments, such as the EBA's Risk Factors Guidelines [34], AML/CFT colleges guidelines[35], the EBA's cooperation guidelines under Article 117 of Directive 2013/36/EU, draft regulatory technical standards (RTS), which are currently being developed by the EBA under Article 9a of Regulation (EU) No 1093/2010 and the amended guidelines on internal governance under Directive 2013/36/EU. Moreover, the guidelines aim to be aligned to international standards (e.g. FATF risk-based approach guidance, Basel Committee on Banking Supervisions (BCBS) guidelines on interaction and cooperation between prudential and AML/CFT supervision, etc.).

9. Generally, the enhanced detail and the greater harmonisation would help competent authorities to operationalise the risk-based approach to AML/CFT supervision, strengthening the level playing field for AML/CFT supervision in the single market.

C. Baseline scenario

10. The ESA's Guidelines on risk-based AML/CFT supervision, published in November 2016 with effective date of implementation by one year after the publication, aimed at ensuring that supervisors take certain steps when implementing their risk-based supervision model.

11. Afterwards, the EBA's report on the competent authorities' approaches to AML/CFT supervision of banks published in February 2020 identified weaknesses in the application of a risk-based approach to AML/CFT supervision. In particular, the report contained recommendations on how competent authorities can address the issues identified in the report and included, among others, recommendations related to the sectoral and subsectoral risk assessments, supervisory strategy and plan, and supervisory cooperation.

12. In order to mitigate the identified weaknesses, the review of the Risk-based Supervision Guidelines will mainly strengthen areas related to cooperation with other competent authorities, risk assessments, supervisory strategy and plan, supervisory tools including follow-up, guidance to the sector and training.

D. Options considered

13. The EBA considered whether the review of the existing guidelines should be tackled through an update or a complete overhaul, and whether the level of detail should be maintained as high-

[33] The supranational risk assessment report is issued under the mandate conferred by Article 6(1) of AMLD4 to update its report every 2 years.

[34] Consultation Paper on the draft guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 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 (JC 2019 87).

[35] Joint guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions (JC 2019 81).

level guidelines with some elements of specific guidance or detailed guidelines with specific examples.

Approach

Option 1: Minor changes to the GLs are introduced

14. These guidelines could adopt the same approach as the original Risk-Based Supervision Guidelines36 with only minor updates and clarifications included where necessary. The first version of the guidelines was developed to fulfil the mandate of Article 48(10) of Directive (EU) 2015/849 to create a common understanding of the risk-based approach to AML/CFT supervision by explaining the characteristics and the steps of risk-based supervision. This option would be the least disruptive to the competent authorities who have already put in place their risk-based supervision models but would be ineffective to address the weaknesses identified in supranational reports and the report published by the EBA summarising findings from the implementation reviews.

Option 2: Substantial changes of the guidelines

15. Substantial changes are included by introducing subsections within already existing parts of the guidelines in those areas where weaknesses were identified (cooperation and information exchange, sources and types of information required for the risk assessment and sectoral, subsectoral, group and individual risk assessments) and by including new sections to the whole structure of the guidelines (supervisory tools, supervisory practices and supervisory follow-up).

16. The Commission in the supranational risk assessment report issued in July 2020 pointed out that the European Banking Authority, pursuant to the Council Action Plan, works on more detailed guidance for the application of the relevant rules. This additional section will provide more detail to supervisors when performing risk-based approach to AML/CFT supervision and provide more clarity to the existing provisions to avoid breaches of the AML/CFT regime.

Option 3: Not to amend the guidelines

17. The EBA implementation review published in February 2020[37] raised the need to review the guidelines in those areas where weaknesses were identified. Therefore, this option would not be desirable in line with the Commission supranational risk assessment report and the EBA implementation reviews.

[36] Joint 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.

[37] EBA report on competent authorities' approaches to the anti-money laundering and countering the financing of terrorism supervision of banks, EBA/Rep/2020/06.

Option 4: Draft a completely new set of the guidelines

18. A complete review of the guidelines would increase the risk of misalignment of the guidelines to the international standards and FATF Recommendation 26 and its interpretative note. Moreover, a complete overhaul could be too disruptive an approach for competent authorities who have already implemented their risk-based approach in line with the existing guidelines.

Level of detail

Option 1: High-level guidelines with some elements of specific guidance

19. This is the approach of the first version of the Risk-Based Supervision Guidelines that provide high-level principles, which are complemented with details in some areas. This approach would represent continuity with respect to the previous guidelines, but would not effectively address weaknesses identified in the implementation reviews carried out by the EBA. In order to strengthen supervisory convergence in the area of AML/CFT supervisions, it is therefore desirable for the guidelines to be a bit more detailed than the level-1 text in respect of some areas.

20. However, taking into account that Directive (EU) 2015/849 is a minimum harmonisation directive that requires Member States to transpose it into their national legislation, allowing them to impose additional requirements where they are justified based on an increased ML/TF risk only a certain level of harmonisation can be achieved through guidelines.

21. This option gives more flexibility to competent authorities to adapt the guidelines to the specific characteristics of different sectors and risks, but it will not contribute towards the harmonisation of specific aspects of the risk-based supervision approach.

Option 2: Guidelines with enhanced level of detail

22. The updated guidelines will provide further details to the previously existing sections and include new sections in those areas with needs of further enhancement. This approach will increase guidance to competent authorities on those areas where weaknesses have been identified and those that would need alignment with other regulatory products recently developed (e.g. cooperation and information exchange), without representing a complete overhaul of all subsections of the guidelines. Moreover, these guidelines should be sufficiently flexible so that they can be applied by AML/CFT supervisors in all sectors[38]. Thus, supervisors should be able to apply these guidelines equally when supervising sectors that are exposed to less significant and very significant ML/TF risks, which may not be possible if the guidelines are too detailed or too prescriptive.

[38] Credit institution or a financial institution as defined in Article 3(1) and (2) of Directive (EU) 2015/849.

23. These additional details would not constrain competent authorities in the process of adapting the supervisory approach to the risk identified in the local markets and across different sectors, but facilitate the work through the additional clarity about the supervisory tools and powers available for them to fulfil an effective risk-based AML/CFT supervision.

E. Preferred option

24. Option 2 is the preferred option.

F. Cost-benefit analysis

25. The implementation of the amended guidelines, which further develop pre-existing provisions and add new ones, entails one-off costs for competent authorities and firms and future costs associated with the evolving adaptation of supervisory practices to the level of ML/TF risk associated with a sector, a particular product or a group of clients.

26. Regarding AML/CFT supervisors, one-off costs are related to carrying out sectoral and subsectoral risk assessment, if not done already, the adaptation of methodologies, supervisory manuals, policies and procedures, and the implementation of the necessary cooperation mechanisms where they do not exist. Moreover, staff should be trained in order to ensure a consistent application of the supervisory tools and practices in line with the supervisory manual. Other future costs are related to the update of the supervisory practices to the evolving conditions of the market and sectors of activity (e.g. increased risk identified in a sector is accompanied by more intensive and intrusive supervisory tools).

27. According to the EBA implementation report published in February 2020, all competent authorities assessed had implemented the risk-based approach to AML/CFT supervision at different levels of maturity. Thus, the additional costs of implementation of the amended risk-based supervision guidelines is expected to be medium.

28. Benefits for AML/CFT supervisors: after developing effective supervisory strategy and plans, they will be able to adjust their resource and supervisory efforts in a more efficient manner by allocating more resources to the supervision of those sectors that are exposed to more significant ML/TF risks. This means that for less-risky sectors supervisors will be able to choose supervisory tools that are less resource intensive, while not sacrificing the effectiveness of their supervision. The new guidelines will also ensure the application of common supervisory practices and the harmonisation of certain terms, make it easier for the competent authorities to cooperate and exchange information with other competent authorities and other stakeholders. Moreover, increased convergence and better understanding of supervisory practices will make it easier for the competent authorities to adjust their practices in future when they will be required to report certain information to the EBA through the database which is currently being created in line with Article 9a of Regulation (EU) No 1093/2010.

29. In the long run, the implementation of these guidelines would potentially lead to more clarity within the market of the supervisory expectations, which could lead to less breaches and shortcomings committed by firms. As a consequence, it would reduce the supervisory measures and sanctions that supervisors should impose and, instead, their focus will be on more effective supervision of more risky firms and sectors and less efforts will be required for the supervisory follow-up actions.

G. Overall impact assessment

30. For the purposes of assessing the level of implementation of the guidelines, we leverage data provided by competent authorities during 2020 for the purposes of the bi-annual Joint Opinion on ML/TF risks affecting the European Union's financial sector published by the EBA under Article 6(5) of Directive (EU) 2015/849.

31. Regarding the policy objective of fulfilling greater harmonisation in the risk assessment process through the use of four ML/TF risk categories[39], less than half of the competent authorities use different risk categorisation. Therefore, the impact of implementing the harmonised risk categories is low, considering the fact that the competent authorities that use national categorisation already have implemented systems to allocate firms within different risk categories.

32. Regarding the methodology for risk assessment, most competent authorities account for a formal risk assessment methodology such as that envisaged in the previous version of the guidelines, in particular for some sectors (e.g. credit institutions, life insurance undertakings, payment institutions and investment firms). Thus, the impact of implementing the additional provisions of risk assessment from an ML/TF perspective (i.e. relating to sectoral and subsectoral risk assessment) is expected to be low.

33. After the implementation of a robust supervisory strategy which is based on competent authorities' risk assessment, those competent authorities that have so far mainly focused on the supervision of banks will need to make adjustments in their supervisory approach to ensure that they also focus on other firms or sectors presenting significant or very significant risk. Equally, those competent authorities that applied no supervision to sectors presenting less significant risk, will also need to adjust their approach to ensure that all subjects of assessment or sectors receive adequate supervision in line with their risk exposure. This means that, in line with the risk-based approach, sectors or subjects of assessment that are less vulnerable to ML/TF may receive less intense or less frequent supervision than the sectors or subjects of assessment that are exposed to more significant levels of ML/TF risk. Thus, the impact of implementing risk-based supervisory tools and practices of the new guidelines is expected to be medium.

[39] Less significant, moderately significant, significant and very significant.

5.2 Feedback on the public consultation and on the response provided by the BSG as part of the consultation

The EBA publicly consulted on the draft guidelines. The consultation period lasted for 3 months and ended on 17 June 2021. Ten responses were received, including a response from the BSG. All the responses were published on the EBA website.

Below is a summary of the key points arising from the consultation. The feedback table that follows provides further details on the comments provided, the EBA's analysis of those comments and the actions taken to address these comments where this was necessary.

Summary of key issues and the EBA's response

Respondents that contributed to the public consultation were asked to provide their responses to the following questions:

- Do you have any comments on the proposed changes to the 'Subject matter, scope and definitions'?
- Do you have any comments on the proposed changes to Guideline 4.1 'Implementing the RBS Model'?
- Do you have any comments on the proposed changes to Guideline 4.2 'Step 1 – Identification of risk and mitigating factors'?
- Do you have any comments on the proposed changes to Guideline 4.3 'Step 2 – Risk assessment'?
- Do you have any comments on the proposed changes to Guideline 4.4 'Step 3 – Supervision'?
- Do you have any comments on the proposed changes to Guideline 4.5 'Step 4 – Monitoring and updating of the RBS Model'?

In the responses received to Step 1, the EBA received suggestions to add examples of possible sources of information as part of the risk identification process, and notably information gathered as part of public-private partnerships (PPPs). The EBA agreed with this suggestion and amended the relevant paragraph in the guidelines to add PPPs in the indicative list of sources of information, if they are available in the jurisdiction.

In the responses received to Step 2, the EBA received a number of comments on the need to clarify further the assessment of the ML/TF risks at the group level and asking for more clarity on supervision of groups at the domestic level and supervision of groups in a cross-border context. The EBA agreed to this and amended Step 3 in relation to group supervision accordingly. In particular, the EBA clarified in the relevant paragraphs that cover group supervision what the expectations are for the supervision of groups at the domestic level on the one hand and for the supervision of

groups operating across borders, on the other hand. For the latter, the EBA detailed further the type of cooperation that is expected and the information that should be shared in that context, in particular the exchange of information related to risk assessment.

In the responses received to Step 3, the EBA received suggestions to clarify situations where off-site reviews should be conducted. The EBA agreed to provide further clarity and has amended the relevant paragraph accordingly, and also aligned it further with the FATF's guidance on the risk-based approach to AML/CFT supervision issued In March 2021.

A fourth set of suggestions related to the assessment by competent authorities in Step 3 of firms' AML/CFT systems and controls was to clarify further how to assess whether AML/CFT systems and controls are effective enough. The EBA amended the relevant paragraphs in order to add, as part of the illustrative list of indicators that may suggest that the AML/CFT framework is implemented effectively, both the systems and processes used to screen customers and transactions and the policies and processes in place to identify and analyse suspicious or unusual transactions and report to the authorities.

Finally, in the course of its work on the preparation of the guidelines on the role, tasks and responsibilities of AML/CFT compliance officers prepared under Article 8 of Directive (EU) 2015/849, the EBA included Guideline 4.4. related to the review of the AML/CFT compliance function by competent authorities.[40] As this guideline was addressed to competent authorities, provisions of Guideline 4.4 were consulted through the draft guidelines on policies and procedures in relation to the compliance manager and the role and responsibilities of the AML/CFT compliance officer, but have been integrated in the revised Risk-based AML/CFT supervision guidelines, in particular in its Guideline 4.4.5.

[40] Consultation Paper on Draft 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.

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

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 was of the view that the definition of 'competent authority' in the list of definitions should be added, despite the fact that it was included in a new section titled 'Addressees' in the guidelines.	The section 'Addresses' makes clear that the guidelines are addressed to competent authorities and makes clear reference to point (2)(iii) of Article 4 Regulation (EU) No 1093/2021. Also, the guidelines clarify that the same definitions as those in the (anti-money laundering directive (AMLD)) should be used. Therefore, it is not necessary to repeat the definitions.	*None*
Section 'Subject matter, scope and definitions'	One respondent suggested that the terminology 'obliged entities' should be kept instead of the proposed term 'subjects of assessment'.	The definition of 'subject of assessment' is not a new addition to the guidelines and was already part of the ESA's Joint Guidelines. The definition was therefore not in the scope of the consultation.	*None*
Section 'Subject matter, scope and definitions'	One respondent expressed concerns about the definition of 'threat' referring to the criminals 'past, present and future ML or TF activities' and suggested a clarification to specify that this refers only to published and publicly accessible reports and information, at least for the obliged entities.	The definition is in line with the approach taken by other international organisations. In addition, the sources of information to be used to assess ML/TF risks are detailed in Section 4.2.2 of the proposed guidelines.	*None*
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 4.1.2. 'Proportionality'	One respondent, while in support of the clarification brought in the draft guidelines, suggested including a reference to the need for a degree of risk tolerance based on a professional evaluation of the entity's risk-based approach.	The proposed guidelines in paragraph 14 make clear that competent authorities are required to implement a supervisory model based on their risk assessment of sectors and subject of assessment.	*None*
	One respondent suggested that the guidelines could further clarify how competent authorities should balance supervisory activities towards institutions with a large number of customers and transactions versus credit and financial institutions (large or small) that pose a high ML/TF risk. Similarly, another respondent in that regard indicated it was not in favour of the removal of the reference to the 'nature and size of the subject of assessment'.	The proposed wording in paragraph 15 makes clear that 'the size or systemic importance of a subject of assessment may not, by itself, be indicative of the extent to which it is exposed to ML/TF risk'. This wording does not imply that the size or systemic importance of a subject of assessment is irrelevant, but instead stresses that small credit institutions or financial institutions that are not systemically important can nevertheless pose a high ML/TF risk.	*None*
Guideline 4.1.3. 'Subjects of assessment'	One respondent suggested that in paragraph 18 of the proposed guidelines, the following should be added: 'Competent authorities should consider whether they will treat credit institutions or financial institutions in the same sector that form part of the same domestic financial group as one "subject of assessment" but should not cluster them. Clustering should be avoided if an institution differs from the other group institutions in terms of its business activities and therefore has a different level of risk than the other institutions in the domestic financial group.'	The definition of 'cluster' makes clear that a cluster means 'two or more credit institutions or financial institutions in a sector having similar characteristics and exposure to the same levels of ML/TF risk'. Therefore, the guidelines are already clear that clustering should be avoided if a credit institution or financial institution in a sector have different characteristics and different exposure to ML/TF risk.	*None*
	One respondent suggested amending slightly the last sentence of paragraph 19 to refer, in addition to changes in products or services, to delivery channels, customers and geographies.	The EBA, having assessed the consultation response, agrees with the suggestion and has amended the relevant paragraph.	*Change introduced in paragraph 19*

	Another respondent acknowledged that while the guideline concerns *domestic* institutions, the EBA could consider clarifying or amending the guidelines to stimulate more coordinated supervisory actions with regard to cross-border institutions.	In accordance with the current legal framework, the AML/CFT supervision is carried out by competent authorities at the national level based on national transpositions of Directive (EU) 2015/849 (AMLD). However, the EBA recognises the borderless nature of financial crime and therefore has introduced a new Guideline 4.3.4, which deals with the supervision of institutions that operate on a cross-border basis. In particular, the guidelines require that the competent authority, which is responsible for the supervision of the head office entity, develop a good understanding of ML/TF risks associated with subjects of assessment that are part of a group and explains what competent authorities should do to understand the risks at group level.	*None*
Guideline 4.1.4 'Cooperation'	One respondent suggested that the EBA could consider mapping the possibilities and restrictions for the cooperation and sharing of information within Member States as well as at the cross-border level.	The AMLD is clear in Articles 49-57 that Member States shall ensure that policy-makers, the FIUs, supervisors and other competent authorities involved in AML/CFT have effective mechanisms to enable them to cooperate and coordinate domestically. The guidelines furthermore provide in Section 4.3.4. clarification on cooperation and exchange of information at group level. Practical modalities for this cooperation are also set out in the EBA's colleges GLs[41] and EBA's GLs on Cooperation (under Art 117 CRD) currently being finalised.[42] As regards information-sharing, the confidentiality and professional secrecy rules applicable to national competent authorities (NCAs) are already set out in the AMLD in Article 48. The AMLD is clear that competent authorities should be able to cooperate and exchange confidential information, regardless of their respective nature or status. In accordance with the Directive, Member States should thus not prohibit or place unreasonable or unduly restrictive conditions on exchange of information.	*None*

[41] EBA's AML/CFT Colleges Guidelines, JC 2019 81.

[42] Consultation paper, Draft Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU, EBA/CP/2021/21.

	With regard to paragraph 20, one respondent suggested clarifying that the various regulators within the same country should avoid duplication of reporting.	Paragraph 48 of the proposed guidelines already provides that when determining the level and frequency of the information requests, competent authorities should consider if information requested is available to the competent authority from other sources, including prudential supervisors, to reduce the duplication of information requests. Furthermore, paragraph 21 makes reference to the ESAs Joint guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions (JC 2019 81), the EBA Guidelines on cooperation and information between prudential and AML/CFT supervisors and financial intelligence units under Directive (EU) 2019/878 and the Multilateral Agreement between the European Central Bank and national competent authorities pursuant to Article 57a(2)(b) of Directive (EU) 2015/849. The latter also provides clarifications on the exchange of information between competent authorities, and also aims to avoid duplication of efforts.	*None*
	Another respondent suggested, in paragraph 20, adding judicial authorities, professional orders and social security institutions as 'potential stakeholders'.	This paragraph was revised to include examples of potential stakeholders with which competent authorities should consider cooperating and does not aim to include an exhaustive list of these stakeholders. However, the EBA sees merit in adding 'judicial authorities' as part of the examples provided in the guidelines and has therefore included it in the relevant paragraph 20.	*Change introduced in paragraph 20 of the revised guidelines*

	Another respondent suggested that references to the guidelines be expanded to also include cooperation with law enforcement authorities and Europol.	The section on cooperation aims to clarify how cooperation can inform risk assessment and the implementation of a RBA. Cooperation between relevant competent authorities are dealt with in complementary guidelines, including those already referred to in the same paragraph. 'Law enforcement agencies' are furthermore already referred to in paragraph 20 of the GLs.	*None*
	With respect to paragraphs 22, 23, 34 and 47 and 48 of the draft guidelines, a respondent suggested that the EBA should clarify to what extent the preamble of the General Data Protection Regulation (GDPR) has been taken into account, as to have a clear basis for the information to be delivered to competent authorities.	AMLD provides in Article 7 that each Member State shall take appropriate steps to identify, assess, understand and mitigate the risks of money laundering and terrorist financing affecting it, as well as any data protection concerns in that regard. Articles 40-44 clarify further the processing of personal data. Article 43 of the AMLD establishes that the processing of personal data for AML/CFT purposes is a matter of public interest under the General Data Protection Regulation, while Article 41 mandates Member States to restrict data subjects' rights to access personal data where this right could interfere with the prohibition of disclosure in Article 39(1) of said Directive. The EBA acknowledges there may be some legal uncertainty associated with the processing of personal data in the AML/CFT context due to the powers of Member States to stipulate further requirements in this area and therefore the EBA in its response to the European Commission's Call for Advice recently recommended that the Commission provide further clarity.	*None*

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 4.2.1. 'General considerations'	One respondent suggested adding in paragraph 24 the following sentence: 'for this purpose consultation may be sought with other public authorities, private entities and other relevant experts' as to further align efforts for fighting (financial) crime at a national or European level. Another respondent underlined that increased cooperation with other authorities could lead to a better understanding of the ML/TF risks by competent authorities, and in particular, as regards the ML/TF of different sectors and subsectors and suggested stressing this further in the guideline.	Paragraph 127 of the draft guidelines already makes clear that competent authorities should engage with subjects of assessment and other relevant stakeholders when developing supervisory guidance, including through a public consultation process, engagement with trade associations, financial intelligence units, law enforcement, other competent authorities or government agencies or through participation in consultative forums. Paragraph 131 also specifies that competent authorities should identify the communication tools available to them and use the most effective tools when communicating with relevant stakeholders. The EBA however sees merits in amending the paragraph to clarify this aspect and the paragraph has been amended accordingly.	*Change introduced in paragraph 126 of the revised guidelines*

Guideline 4.2.2. 'Sources of information'	In paragraph 31, two respondents suggested adding 'Public Private Partnerships' (PPPs) as a source of information.	The EBA, having assessed the consultation response, agrees with the suggestion and has amended the relevant paragraph 31c.	*Change introduced in paragraph 31 of the revised guidelines*
	In paragraph 31, one respondent suggested that 'newspaper reports' should have been kept in the guidelines, instead of replacing it with 'publicly available information from reputable sources'. The same respondent also pointed out that the term 'reputable source' can be interpreted widely and that the guidelines do not provide sufficient clarity on what could be perceived as 'reliable information'.	This amendment to the guidelines was made in line with the revised EBA's guidelines on AML/CFT Risk Factors Guidelines, which require that information be gathered from reputable sources. The relevant paragraph 31 has however been amended slightly to provide further details, in line with the EBA Risk Factors Guidelines.	*Change introduced in paragraph 31 of the revised guidelines*

	In paragraph 33, one respondent suggested making reference to other typologies of offences when referring to the connection between predicate offences and money laundering.	The EBA, having assessed the consultation response, has amended paragraph 33 to clarify further the need to consider relevant typologies and predicate offences.	*Change introduced in paragraph 33 of the revised guidelines*
	Another respondent underlined that the removal of the reference to information from 'private entities' is unconvincing and therefore suggested replacing the proposed term 'relevant bodies' with 'credible private bodies and other relevant bodies'.	The revision was made to take into consideration that the reliability of information supplied by a private entity may be called into question. The proposed wording ('relevant bodies') is wide enough to include private bodies, among others. However, the EBA has introduced an amendment to address this comment in 33d).	*Change introduced in paragraph 33 of the revised guidelines*
Guideline 4.2.5. 'Sector-wide ML/TF risk factors'	One respondent suggested adding a reference to the Bauspar sector (i.e., building societies specialised in saving and real estate financing) as a subsector in paragraph 38.	The proposed guidelines are already clear that competent authorities should consider subdividing sectors into subsectors and refer to money-remitters, private banks, and brokerage firms as examples of subsectors of payment institutions, credit institutions and investment firms, respectively. The intention in this paragraph is not to provide an exhaustive list of all existing subsectors that in addition may differ across the EU.	*None*

Guidelines 4.2.6. 'Type of information necessary to identify risk factors'	One respondent suggested clarifying that information gathered by competent authorities should be shared with the subject of assessment.	In the section 'Communication with the sector', paragraphs 130 and 132(c), the proposed guidelines already make clear that competent authorities should ensure that the required information relating to the risk assessment is made available to subjects of assessment in a timely manner. Furthermore, most of the necessary information is gathered from the subjects of assessment through various supervisory engagements with them, including AML/CFT returns and inspections, and the outcomes of the risk assessment will be shared with them. As regards other information, NCAs are not allowed to share any non-public information.	*None*
	One respondent suggested clarifying in paragraph 41(j): 'threat reports, alerts and typologies from financial intelligence units and other responsible state institutions if applicable'.	The EBA, having assessed the consultation response, has amended paragraph 41(j) accordingly.	*Change introduced in paragraph 41(j) of the revised guidelines*
	Another respondent suggested making clear in paragraphs 43–48 that for the purpose of collecting all the necessary information, competent authorities should coordinate closely with prudential supervisors to prevent overlapping. As an example, the annual AML supervisory programme should be approved by all supervisors.	The proposed guidelines already make clear in paragraph 43 that competent authorities should gather sufficient, relevant and reliable information from the sources described in paragraphs 30 and 31, which include supervisory authorities responsible for the supervision of subjects of assessment' compliance with prudential requirements. Furthermore, in accordance with the AMLD, the AML competent authorities are responsible for setting their supervisory programme on a risk-sensitive basis. Therefore, the GLs encourage cooperation between supervisors, however the responsibility for the Supervisory programme rests solely with the AML supervisors.	*None*

	Another respondent suggested including a distinction in paragraph 44 (d) in relation to the technology used to provide services through non-face-to-face channels. In particular, the respondent is of the view that controls applied in some identification and verification technologies should be considered as an equivalent to face-to-face onboarding.	The AMLD is technology neutral and so are the EBA guidelines. The EBA's ML/TF Risk Factors Guidelines in that regard include a section on customer due diligence (CDD) in non-face-to-face situations, including in situations where innovative CDD solutions are being used (see Guidelines 4.29 to 4.37 of the guidelines).	*None*
	Another respondent, in relation to paragraph 44(e), suggested including a reference to the subjects who have recently ceased to be qualified as PEPs (e.g. subjects who were qualified as PEPs in the last year, but who are no longer considered so) and subjects who are strictly connected to PEPs (e.g. PEPs' family members). The respondent also suggested that the current paragraph should also include a reference to customers that are not strictly qualified as 'PEPs', but who have a relevant political role (e.g.: mayors of cities with more than 15.000 habitants).	The AMLD clearly defines who is a PEP in its Article 3, including what concerns family members. The Directive is furthermore clear that Member States should determine who qualify as prominent public function holders in accordance with national laws, regulations and administrative provisions. Obliged entities are responsible for identifying ML/TF risks associated with their business, including their customers and, in order to help them in this task, the EBA has published the Risk Factors Guidelines[43] that address situations where the customer may present heightened ML/TF risks	*None*
	Another respondent suggested that paragraph 47 should include an explicit reference to the 'proportionality' of the request of data to individual subjects of assessment and therefore should be amended as follows: '…competent authorities should ensure that the amount and the type of information requested are proportional and determined by…'.	Paragraph 14 of the proposed guidelines already provides that competent authorities should be proportionate in their supervision of subjects of assessment for AML/CFT purposes and that the extent of information sought, and the frequency and intensity of supervisory engagement and dialogue with a subject of assessment should be commensurate with the ML/TF risk identified. Equally, paragraph 48 is clear that competent authorities should consider adjusting the level and frequency of information requested from subjects of assessment based on the level of the risk associated with the sector or subsector to which the subject of assessment belongs.	*None*

[43] EBA's ML/TF Risk Factors Guidelines, EBA/GL/2021/02

	Another respondent suggested, in relation to paragraph 47 and 48, that the EBA provide further clarification that supervisors that are part of an AML/CFT college for a specific institution, should coordinate their requests, preferably by agreeing on the set of information needed, the time interval, as well as the format.	In the ESAs' AML/CFT Colleges Guidelines (JC 2019 81), Guideline 12 and 13 provide the basis for a common approach to the AML/CFT supervision of the firm and sets out the process that permanent members should follow to ensure the effective and consistent oversight of the group. Guideline 13 furthermore sets out a process for coordinated supervisory actions.	*None*

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. 'Assessment of the ML/TF risks	One respondent, referring to paragraphs 60-62, would welcome further reference to coordination by competent authorities, preferably by coordinated supervisory inspections, with coordinated reporting requirements and formats.	In the ESAs' AML/CFT Colleges Guidelines (JC 2019 81), Guideline 12 and 13 provide the basis for a common approach to the AML/CFT supervision of the firm and sets out the process that permanent members should follow to ensure the effective and consistent oversight of the group. Guideline 13 furthermore sets out a process for coordinated supervisory actions.	*Change introduced in paragraph 95 of the revised guidelines*

at the group level'		However, the EBA sees merit in providing further clarification on group supervision and had amended the guidelines that cover supervision, also in line with another comment received in this section (see below).	
	One respondent was of the view that the risks arising from the subject of assessment's exposure to countries are not limited to the factors analysed in paragraph 60(a)-(e) and suggested that the current list of foreign risk factors should also include a reference to 'countries or territories that have been subject to sanctions, embargo or similar measures adopted by national or international competent authorities'.	Paragraph 60c), d) and e) cover the situations that competent authorities need to reflect on in their risk assessment. The EBA revised risk factors guidelines, on the other hand, include in the risk factors what firms should consider when identifying the level of terrorist financing risk associated with a jurisdiction, the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union. The EBA, having assessed the consultation response, has amended paragraph 60d to provide further clarification.	*Changes introduced in paragraph 60(d) of the revised guidelines*
	Referring to paragraph 61, one respondent suggested clarifying the interaction between the AML/CFT colleges and third countries.	The ESAs' AML/CFT Colleges Guidelines (JC 2019 81) already provide that AML/CFT colleges provide a permanent structure for cooperation and information exchange between supervisors from different Member States and third countries that are responsible for the AML/CFT supervision of the same firm. Guideline 5.4. specifies that the AML/CFT authorities and prudential supervisors of third countries where cross-border establishments operate can be invited to the AML/CFT college as observers, subject to meeting relevant confidentiality and professional secrecy requirements.	*None*
	Referring to paragraph 62, two respondents suggested providing further clarification on the criteria that could be used to assess an effective implementation of group-wide policies and procedures in branches and subsidiaries of subjects of assessment.	Paragraph 100c of the proposed guidelines provide a list of indicators competent authorities should consider when assessing effectiveness within the subject of assessment. Some of these criteria are also relevant at group level. The ESAs' AML/CFT Colleges Guidelines (JC 2019 81) furthermore clarify the practical modalities of supervisory cooperation and information exchange to create a common framework that supervisors should use to support effective oversight of cross-border groups from an AML/CFT perspective. Further details have also been added in paragraph 96 of the guidelines.	*None*

Guideline 4.3.5. 'Weighting risk factors'	One respondent suggested adding to paragraph 63(d) an additional explanation to make clear that competent authorities should ensure that one risk factor does not sway automatically the balance of the overall weighting to a disproportionate and unreasonable assessment, when the risk factor does not imply a higher ML/TF risk.	Paragraph 63(d) is already clear that weighting should not be unduly influenced by just one risk factor and that when weighting risk factors, competent authorities should ensure that one risk factor does not sway the balance of the overall weighting to a disproportionate and unreasonable assessment.	*None*
Guideline 4.3.6. 'Risk profiles and categories'	One respondent, with regard to paragraph 67, suggested a deadline of 30 days to be imposed on competent authorities to assign the residual risk score when the relevant information becomes available.	The proposed guideline 4.5.1 'Review of the risk assessment and supervisory strategy and plans' already provides guidance on when competent authorities should review their risk assessment, including on an ad hoc basis. The guidelines make clear in paragraph 138 that risk-based supervision is not a one-off exercise, but an ongoing and cyclical process and that competent authorities should carry out periodic or ad hoc reviews of the information on which their risk assessment is based, and update this information as necessary.	*None*
	One respondent suggested ensuring that a common understanding on risk profiles and categories is adopted in order to achieve convergence and enhance cooperation.	Paragraph 70 of the proposed guidelines provides that when categorising the inherent risk associated with subjects of assessment, sectors or subsectors, competent authorities should consider the following four risk categories: less significant risk, moderately significant risk, significant risk, very significant risk. To enable the comparison between different risk categories, the proposed guidelines furthermore contain an annex in which the EBA provides further guidance on conversion of risk categories, which should be used when the competent authority has, as part of its risk assessment methodology, adopted the risk categories that are different from those listed in the guidelines. This is in line with the risk categories used across the EBA's regulatory instruments and also in line with the European Commission's supranational risk assessment (SNRA) published in 2019.	*None*

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**
4.4.1. 'General provisions'	Referring to paragraph 75(c), one respondent suggested further clarifying how a competent authority should form their supervisory plan when balancing different types of institutions in terms of size, type of business activities and exposure to more significant ML/TF risks.	The Guidelines are clear that, in order to develop an effective risk-based supervision framework, competent authorities are required to identify and assess institutions' exposure to ML/TF risks. This aspect is detailed in Step 2 of the Guidelines. Thereafter, based on the risk assessment carried out in Step 2, competent authorities are required to develop a strategy setting out how they will supervise each risk category over a certain period of time. In paragraph 78, the guidelines explain that as part of their strategy, competent authorities are required, among other things, to identify supervisory tools that they plan to apply to each risk category on a cyclical basis. In accordance with para. 79, competent authorities then implement their supervisory strategy in practice through their supervisory plans, which may be annual, bi-annual or for another duration. Competent authorities should keep track of all supervisory plans in respect of subjects of assessment to ensure that together they fulfil the strategy. To provide further clarifications on the supervisory plans, paragraph 78-79 was amended slightly.	*Change introduced in paragraph 78-79 of the revised guidelines*
	On respondent suggested adding to paragraph 78: '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 pre-established timeframe'. The same respondent also recommended adding the following points to the list of six elements a) to f) under paragraph 78: - Ensure that supervisory objectives are expressed in terms of outcomes and/or impacts rather than outputs or inputs.	The EBA agrees that the reference to a specific timeframe would be valuable and has amended the relevant paragraph. As regards the suggested reference to outcomes and/or impacts rather than outputs or inputs, the EBA does not see the need for amending the guidelines. Paragraph 78 is already clear that competent authorities should set clear objectives for their approach to AML/CFT supervision and set out how these objectives will be achieved.	*Changes introduced in paragraph 77 and paragraph 156 of the revised guidelines*

	- Establish a systematic approach to monitor and report on progress towards the supervisory objectives set out in the strategy. - Determine qualitative and quantitative indicators linked to the supervisory objectives, together with the baseline and target values for those indicators within the relevant timeframe.	As regards the suggestion to refer to an approach to monitor and report on progress towards the supervisory objectives set out in the strategy, the EBA agrees that this would be valuable and has introduced changes in the relevant paragraph. As regards the suggestion to make reference to qualitative and quantitative indicators linked to the supervisory objectives, the guidelines are already clear that competent authorities should determine and implement an AML/CFT supervisory strategy where they set out how they will mitigate the ML/TF risks they have identified.	
	Referring to paragraph 78(b), a respondent was of the view that supervisory coverage and monitoring commensurate with the ML/TF risk has to be applied to all sectors and subsectors, regardless of the risk level. The respondent thus suggested that the reference to 'including those associated with lower ML/TF risk' is redundant and should be removed.	The EBA agrees with the respondent that all sectors and subsectors should be covered regardless of their exposure to ML/TF risks and it is confirmed by the guidelines in paragraph 78(b). Nevertheless, the EBA considers it necessary to retain the reference to the low risk firms in this paragraph to remind competent authorities of their responsibilities also in respect of low risk sectors because the EBA, through its implementation reviews of competent authorities' supervisory practices[44], has observed that these sectors are often overlooked in practice.	*None*
Guideline 4.4.4. 'Supervisory tools'	A respondent noted that in paragraph 86 the guidelines refer to the 'end goal' whereas in the same paragraph reference is made to the 'purpose'. The respondent therefore suggested more consistency across the guidelines.	To ensure consistency, the EBA has amended the paragraph accordingly.	*Change introduced in paragraph 87*
	With regard to paragraph 87, one respondent suggested that the reference to 'such situation may arise where the competent authority has identified through AML/CFT returns or other supervisory activities an emerging ML/TF risk' was redundant, could be misinterpreted and as a result should be removed.	The reference was introduced by the EBA to provide an example of a situation where competent authorities should exercise flexibility and adapt their use of supervisory tools. To clarify that this is provided as an illustration, the EBA has amended paragraph 88.	*Change introduced in paragraph 88*
	With regard to paragraph 87 and in relation to the identification of emerging risks, a respondent noted that supervisors may need to take additional steps to understand the risk profile in relation to firms and activities outside the regulatory perimeter for	As regards potential ML/TF risks arising from non-financial institutions/activities, the EBA would like to emphasise that the risk-based supervision guidelines should be read in conjunction with the EBA's risk factor GLs, where the EBA has identified, among	*None*

[44] EBA Report on competent authorities' approaches to AML/CFT supervision of banks, EBA/Rep/2020/06.

	financial services to which regulated firms provide services, or to understand emerging issues in firms where requirements prior to registration may be more limited than those in place for others requiring authorisation or which are not supervised for non-AML purposes. Where these firms are customers of regulated financial institutions their risk profile may have a wider impact on the financial sector.	other risks, ML/TF risks also associated with certain unregulated activities or services/products like crowdfunding and cryptocurrencies. Furthermore, the EBAs' Opinion on the ML/TF risks affecting the Union's financial sector published in accordance with Article 6(5) of Directive (EU) 2015/849 identifies key emerging ML/TF risks, including those emerging in unregulated services, on a bi-annual basis.	
	Referring to paragraph 88, while the respondent agreed that competent authorities should exercise flexibility in order to carry out ad hoc inspections, a respondent noted that the reference to 'specific event' should be specified, in order to establish when ad hoc inspections should be carried out. To that end, the respondent suggested that the paragraph should be amended as follows '… such inspections may be triggered by a specific event, such as new products or services, new delivery channels of the services or products, different types of customers or new geographic areas where the services or products are delivered...'.	The EBA agrees that further clarification would be beneficial in this paragraph and therefore has amended the relevant text in the guidelines to emphasise the link between the risk exposure of the sector, sub-sector or subjects of assessment and the level of supervision applied to them. This means that, for example, new products or services in itself will not trigger an ad hoc inspection, if it does not increase the ML/TF risk exposure of the financial institution.	*Change introduced in paragraph 93 of the revised guidelines*
	With regard to paragraph 89, a respondent was of the view that competent authorities should determine not only the type and frequency of the supervisory tools used, but also the intensity and intrusiveness of these tools. To that end, the respondent suggested amending the paragraph as follows: 'Competent authorities should recognise that each subject of assessment, sector or subsector is exposed to different levels of ML/TF risk, which should determine the type, frequency, intensity and intrusiveness of the supervisory tools used'.	The guidelines already make it clear that in order to carry out the AML/CFT supervision effectively, competent authorities are required to adjust the frequency, intensity and intrusiveness of AML/CFT supervision on a risk-sensitive basis, but the EBA sees merit in reiterating this point in paragraph 89 (now 90 following above changes). As a result, the EBA has amended the relevant paragraph.	*Change introduced in paragraph 87 of the revised guidelines.*
	With regard to paragraph 91, a respondent noted that the reference to 'When the implementation of AML/CFT systems and controls by subjects of assessment is not the competent authority's key objective' could be misinterpreted, because the current paragraph does not provide a definition of 'competent authority's key objective'. To that end, the respondent suggested that the paragraph should be amended as follows: 'When a full-	Having assessed the comment and to align further with the FATF guidance on risk-based supervision issued in March 2021, the EBA has amended the relevant paragraph.	*Change introduced in paragraph 92 of the revised guidelines.*

	scope on-site inspection is not required, according to par. 90, competent authorities should consider the use of off-site reviews'. Similarly, another respondent suggested clarifying in which situations would it be acceptable for implementation of AML/CFT systems and controls not to be an authority's key objective.		
	Referring to paragraph 93(b), a respondent suggested that reference should be added to the intensity and intrusiveness of the information required. To that end, the respondent suggested that 93(b) should be modified as follows: '…what type of information and which intensity and intrusiveness is needed and how to obtain it effectively'.	The EBA considers that the 'intensity' of the information in many situations cannot be anticipated, as this would depend on the subject of assessment. However, to clarify this paragraph further, the EBA has amended the relevant paragraph accordingly.	*Change introduced in paragraph 91(b) of the revised guidelines*
	Referring to paragraph 96, a respondent noted that cooperation may include exchanging information related to weaknesses or breaches identified by other competent authorities and was of the view that this provision could potentially cause breaches to national data protection laws. Therefore, competent authorities should consider clarifying the scope and means of their cooperation through ad hoc MoUs.	The Financial Action Task Force recognises the cooperation and the exchange of information between competent authorities as one of the key components of effective supervision. To that end, Directive (EU) 2015/849 sets clear expectations for competent authorities to cooperate with each other to the fullest extent and to exchange information necessary for them to carry out their supervisory activities, including information on breaches and weaknesses identified within the financial institution. In general, the information exchanged relates to the financial institution, however, where data or information relating to individuals is exchanged, Directive (EU) 2015/849 requires for it to be exchanged in accordance with the applicable data protection rules. Regarding the scope of the cooperation, the EBA has clarified the scope in Guideline 9 of the AML/CFT Colleges Guidelines[45]. Overall, the level-1 text together with the AML/CFT Colleges Guidelines provides sufficient basis for cooperation and therefore MOUs are not necessary.	*Change introduced in paragraph 95 of the revised guidelines.*

[45] ESAs joint guidelines (JC 2019 81) on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions ('the AML/CFT Colleges Guidelines').

		To that end, the EBA has amended the relevant paragraph slightly to provide further clarifications.	
Guideline 4.4.5. 'Supervisory practices and the supervisory manual'	Referring to paragraph 98, two respondents were of the view that the current formulation seems to indicate that there are two distinct assessments of systems and controls, and only one of those assessments is focused on 'effectiveness'. The respondents underlined that the assessment should be focused wholly on effectiveness.	The EBA considers that competent authorities should consider both the adequacy of systems and controls put in place by the subject of assessment and how effective they are. The EBA has amended the relevant paragraph to clarify this further.	*Change introduced in paragraph 95 of the revised guidelines*
	Two respondents suggested that in the list of factors used to assess effectiveness outlined in paragraph 100, references should be made to: • the provision of useful information to relevant government agencies in defined priority areas; • suspicious activity reporting; • FIUs' views and/or evaluations of the reporting quality coming from financial institutions; • the financial institution's participation in PPPs aimed at improving the detection, disruption and deterrence of financial crime. Furthermore, one of the two respondents suggested that financial institutions and their financial crime compliance programmes should be assessed mostly on the basis of their ability to prevent, detect, and report suspicious activity, rather than focusing on mere technical compliance with regulatory guidance or supervisory expectations. The same two respondents noted that paragraph 100(d) appeared to contain a typo that makes it unclear whether more information following 'business-wide risk assessment' was intended to be included.	Having assessed the suggestions made, the EBA has amended the relevant paragraph, in particular in f). Regarding paragraph 100 d), the EBA has corrected the typo.	*Changes introduced in paragraph 100*
	Referring to paragraph 100 and 101, one respondent noted that when developing the supervisory manual, competent authorities should pay attention to the proportionality principle and the differences between the various subjects of assessment, such as	The EBA considers that this aspect is covered in the steps related to risk assessment that makes it clear that competent authorities should gather the necessary information that allows them to	*None*

	the number and type of products and services and the number and type of customers and transactions.	understanding the subjects of assessment's exposure to customer, products and services, geographical and distribution channel risks. In addition, the proportionality principle is an overarching principle applicable in all stages of the supervisory process as set out in paragraphs 14 and 15 of the guidelines.	
Guideline 4.4.8. 'Supervisory follow-up'	Referring to paragraph 118, one respondent, while agreeing that competent authorities should be able to challenge the remediation plan adopted by the subject of assessment, was of the view that the remediation plan should be challenged not only where the timeline – for when the remediation will be complete – is unrealistic, but also where the remediation steps that have been set out are not suitable or enough to adjust the weaknesses. The respondent thus suggested amending the paragraph as follows: 'the remediation plan should set out a clear timeline for when the remediation will be complete, which should be challenged by the competent authority where the timeline is unrealistic or the remediation steps are not appropriate to the specific weakness'.	The EBA agrees with the suggestion and has amended the relevant paragraph.	*Change introduced in paragraph 116 of the revised guidelines*
Guideline 4.4.9. 'Feedback to the sector'	Referring to paragraph 122-132, one respondent noted that for an effective supervision and efficient implementation of the AML/CFT rules, it was in its view essential that competent authorities transparently communicate to the subjects of assessment the outcomes of their risk assessment (including that of the sector) and provide non-binding guidance to the obliged entities with concise, precise and clear provisions on what they expect them to do to comply with their AML/CFT obligations. The respondent was also of the view that competent authorities should be available for a constructive dialogue with the obliged entities and their representation bodies, and they should consult them before developing official supervisory guidelines in a publicly available way.	The EBA agrees with the respondent that the feedback and communications with the sector are important and have a significant impact on the levels of compliance within the sector. To that end, the Guidelines contain a separate Section 4.4.9 'Feedback to the Sector', which, in the EBA's view, provides comprehensive guidance on how and when competent authorities should communicate with the sector. However, the EBA has now emphasised the importance for the guidance to be clearly communicated to the sector and has amended the relevant paragraph accordingly.	*Changes to paragraphs 129-131 of the revised guidelines*
	Referring to paragraph 122-123, one respondent was of the view that feedback to the sector is not provided in a timely manner and as a result would welcome further clarifications in the guideline as regards the timeline for feedback to the sector. The respondent suggested adding a reference to a more continuous	The EBA agrees with the respondent that any guidance should be communicated to the sector in good time, however, the need for additional guidance is often triggered by certain events, which are impossible to predict, therefore, setting out explicit timelines in	*Changes to paragraph 100 of the revised guidelines.*

	dialogue on the remedial actions between the competent authority and the subject of assessment.	these guidelines for the communication of the feedback is not possible. However, the EBA recognises that supervisory expectations are also communicated to subjects of assessment through findings from inspections or reviews and, indeed, it should be done in a timely manner. Therefore, the EBA has included an additional requirement in the relevant paragraph. As regards the follow-up, this aspect is covered in Section 4.4.8, which is dedicated to the supervisory follow-ups. This section acknowledges that supervisory tools or measures should be proportionate to the materiality of weaknesses and seriousness of breaches identified and take into consideration the level of risk to which the subject of assessment is exposed and specifies in the relevant paragraph that competent authorities should establish a timeline and a description of the concrete supervisory follow-up actions and measures to be taken by the subject of assessment to address each breach or weakness.	
	One respondent, with regard to paragraph 124, was of the view that, in issuing such guidance, supervisors should assess the position of multinational companies vis-à-vis the regulatory framework of third countries. Therefore, this guidance should take into account third countries' regulatory and supervisory expectations, in order to ensure a level playing field in cases when local expectations diverge from the European expectations.	The EBA is mandated to publish this guidance in accordance with Article 48(10) of Directive (EU) 2015/849 and therefore the scope of these guidelines is determined by the Directive. This means that the respondent's suggestion is outside the scope of these guidelines. However, the guidelines aim to foster the engagement between the EU and third-country supervisors by emphasising the importance of cooperation between them as set out in Section 4.1.4. This also includes cooperation and information exchange in AML/CFT colleges where relevant third-country supervisors can be invited as observers. Also, paragraph 22 highlights the need to identify foreign risk factors in respect of sectors and the guidelines also make clear that competent authorities would benefit from knowledge sharing with foreign authorities, such as other countries' AML/CFT supervisors.	*None*

	Referring to paragraph 125(c) and in relation to de-risking, two respondents suggested that competent authorities, when assessing de-risking, should also take into account and recognise the efforts made by financial institutions to build appropriate control frameworks to proactively engage with the 'at risk' clients in order to prevent financial exclusion. Referring to the same paragraph 125(c), another respondent recommended including a reference to consider the need for greater supervision of regulated customer segments, such as Money Services Businesses (MSBs).	The EBA has clarified in its Risk Factors Guidelines[46] that firms should put in place appropriate and risk-sensitive policies and procedures to ensure that their approach to applying CDD measures does not result in unduly denying legitimate customers access to financial services. As regard MSBs, the guidelines already make clear that competent authorities, when assessing risks associated with the sectors under their supervision, should refer to a number of sources, including the bi-annual EBA Opinion on ML/TF Risks, which has a specific section dedicated to payment institutions and e-money providers.	*None*
	Referring to paragraph 126(c), one respondent suggested adding a reference to the EBA revised ML/TF Risk Factors Guidelines, which clarify that the application of a risk-based approach to AML/CFT does not require financial institutions to refuse, or terminate, business relationships with entire categories of customers that are considered to present higher ML/TF risk. Instead, the Guidelines should provide guidance on the steps financial institutions should take effectively to manage ML/TF risks associated with individual business relationships.	The EBA agrees with this suggestion and has amended the paragraph to add a reference to the EBA's Risk Factor Guidelines and in particular in Guidelines 4.9., 4.10. and 4.11.	*Change introduced in paragraph 126 of the revised guidelines*
	Referring to paragraph 129, one respondent suggested adding an explicit mention of the resources required in order to implement the communication strategy, e.g. '...apply a communication strategy, including sufficient human and technical resources, that ensures that…'.	The EBA considers that the paragraph is sufficiently clear and requires that competent authorities should ensure the best use of their supervisory resources.	*None*
Guideline 4.4.10. 'Training of competent authority's staff'	One respondent suggested adding a reference to training on RegTech and risk-based approaches to compliance.	This is already covered in paragraph 135 that makes clear that competent authorities should ensure that their supervisors are trained in the practical application of their AML/CFT RBS Model and have developed a good understanding of different products, services and financial instruments, and the risk associated with them. However, the guidelines are clear that each competent authority is responsible for identifying the training needs within	*None*

[46] EBA's ML/TF risk factors Guidelines, EBA/GL/2021/02.

		their authority and ensuring that staff receive the necessary training, which may also include training on RegTech or any other areas.	
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 4.5.1. 'Review of the risk assessment and supervisory strategy and plans (Steps 1, 2 and 3)'	Referring to paragraph 143(f) on ad hoc review, one respondent was of the view that the current paragraph should also consider that significant changes affecting the subject of assessment's risk profile could be determined not only by a 'sudden change to the customer base', but also by a 'sudden change to the services or products delivered or in the delivery channels or in the geographic areas where the services and products are delivered'. To that end, the respondent suggested amending paragraph 143(f) as follows: 'sudden changes to the customer base, services and products delivered, delivery channels and geographic areas where services and products are delivered, within the sector or sub-sector'.	The EBA agrees with this suggestion and has amended the relevant paragraph.	*Change introduced in paragraph 142(f) of the revised guidelines*
	Referring to paragraph 143(h), one respondent suggested, in order to further ensure legal certainty, to add the following: 'Other situations where the competent authority has reasonable and justifiable grounds to believe that information on which it had based its risk assessment is no longer relevant or has significant shortcomings'.	The EBA agrees with this suggestion and has amended the relevant paragraph.	*Change introduced in paragraph 142(h)*