EBA/GL/2021/16 (consolidated version)

16 December 2021

➢O

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

	Application date
➢O	04.07.2022
Amended by:	
➢A1 EBA/GL/2023/07	30. December 2024
➢C1 EBA/Corrigendum/2023/01	----------

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[1]. 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 30.05.2022. 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).

[1] 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

A1

5. These guidelines specify in accordance with Article 48(10) of Directive (EU) 2015/849[2] and Article 36(3) of Regulation (EU) 2023/1113[3] 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.

O

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

A1

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

O

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.

[2] 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).

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

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.
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 [30.06.2022].

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'.

A1

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; or
    - the credit institution's or financial institution's internal control framework is deficient which has an impact on the credit institution's or financial institution's residual risk rating; or
    - the credit institution or financial institution has introduced significant changes to its products or services, or may have combined those changes with changes in delivery channels, its customer base or different geographic areas where the services or products are delivered.

    When assessing these points, competent authorities should take into account suitability assessments made under the prudential frameworks, in particular, where applicable, assessments in relation to the suitability of members of the management body and of the heads of internal control functions, including those assessments made under the joint ESMA and EBA 'fit and proper' guidelines[4] and the EBA Guidelines on internal governance[5]. In the case of crypto-asset service providers, competent authorities should consider applying Sections 1, 2, 3 and 5 of Title II, Section 6 of Title III, Sections 8 and 9 of Title IV and Title V of the EBA Guidelines on internal governance for investment firms[6] for AML/CFT purposes[7].

O

[4] 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.

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

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

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

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.

C1

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 exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions, [8] the EBA Guidelines on cooperation and information between prudential and AML/CFT supervisors and financial intelligence units under Directive (EU) 2013/36[9] and the Multilateral Agreement between the European Central Bank and national competent authorities pursuant to Article 57a(2)(b) of Directive (EU) 2015/849.[10]

A1

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

O

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

[8] 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.

[9] 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

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

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 with individual business relationships and occasional transactions under Articles 17 and 18(4) of Directive (EU) 2015/849.[11]

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.

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

4.2.2 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:

C1

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

b) the EBA's Opinion on the ML/TF risk affecting the Union's financial sector published in accordance with Article 6(5) of Directive (EU) 2015/849;

c) 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;

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

e) national and foreign governments;

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

g) other competent authorities;

h) AML/CFT supervisory authorities in third countries;

i) 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;

j) the financial intelligence units (FIUs);

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

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

m) 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')[12], where established.

O

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;

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;

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

A1

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

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

O

[12] 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)

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[13] 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

A1

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 categorise obliged entities in line with the list of institutions provided in the definition of credit and financial institutions under Article 3(1) and (2) of Directive (EU) 2015/849.

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. Examples of subsectors include money-remitters, private banks, brokerage firms, and crypto-asset exchanges, which represent subsectors of payment institutions, credit institutions, investment firms, and crypto-asset service providers respectively. To inform their view on sectors and subsectors and their specific features, competent authorities should refer to Title II of the EBA's AML/CFT Risk Factors Guidelines.

O

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

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.

C1

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:

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

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

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

    d) 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;

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

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

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

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

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

A1

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

O

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;

A1

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

O

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;

A1

f) the geographical area of the business activities, in particular where they involve high-risk

third countries[14], including, where 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;

O

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;

A1

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

O

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

[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.

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;

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

C1

51. Competent authorities should develop a good understanding of the 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.

O

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:

A1

    a) that the AML/CFT systems and controls listed in Articles 8(4) and 19a of Directive (EU) 205/849 are put in place and applied. These controls should be sufficiently

comprehensive and commensurate with the ML/TF risks;

- o

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[15], 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[16], 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

[15] (JC 2019 81).

[16] 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.

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 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;

A1

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

O

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.

A1

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

O

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 [17] 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.[18] 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.

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.

[17] 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.

[18] 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

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.[19] 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 [20] 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 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,[21] competent authorities should cooperate with prudential supervisors during the initial assessment and also during any reassessments of suitability by prudential supervisors as necessary.[22] 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:

C1

[19] 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.

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

O

[21] 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.

[22] 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

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;

C1

b) possible instances where supervisors are required to cooperate with other stakeholders as described in Section 4.1.4. of these Guidelines and explain the process of how this cooperation should happen in practice;

O

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:

A1

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

O

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;

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[23] 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;

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

[23] 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.

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[24] 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.

A1

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 with and exchange information on and, where necessary, coordinate actions with respect to the subject of assessment's failures with prudential supervisors.

O

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 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

[24] 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

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;

A1

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

O

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:

A1

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

b) does not directly or indirectly foster or condone unwarranted de-risking of entire categories of customers in accordance with the Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services under Directive (EU) 2015/849 and the EBA's ML/TF Risk Factor Guidelines and in particular guidelines 4.9., 4.10. and 4.11[25];

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

127. Competent authorities should consider engaging with subjects of assessment and other relevant stakeholders when developing supervisory guidance and should determine the

[25] 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.

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

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

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.

A1

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

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

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

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

O

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;

A1

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

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

O

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;

A1

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

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'. Where necessary and appropriate, competent authorities should also consider filling existing knowledge gaps through strategic hires or draw on the support of in-house specialists such as IT specialists.

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

foreign authorities, such as prudential supervisors, the FIU, relevant EU bodies, and other countries' AML/CFT supervisors.

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:

A1

a) professional and technical expertise;

O

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