EBA/CP/2025/12

8 July 2025

Consultation Paper on

EBA Draft Guidelines

on the sound management of third-party risk

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 08.10.2025. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the EBA website.

2. Executive summary

Over recent years, financial entities have been increasingly interested in using third-party service providers (TPSPs) to access specialised expertise, reduce costs, improve scalability, efficiency and focus on core activities. However, reliance on third-party may also increase risks and may expose financial entities, their customers and, in some cases the wider financial system to significant harm. This increased reliance on TPSPs requires an evolution of the traditional notion of outsourcing to the broader scope of TPSP arrangements. In this context, it is necessary for financial entities to continue to effectively strengthen their governance arrangements including their operational resilience.

Directive 2013/36/EU (CRD) strengthens the governance requirements for institutions and Article 74(3) CRD gives the EBA the mandate to develop guidelines on institutions' governance arrangements. Third-party arrangements are one of the specific aspects of institutions' governance arrangements. Directive 2019/2034/EU (IFD) also sets out requirements for internal governance of investment firms which are not considered to be small and non-interconnected and give the EBA, in consultation with ESMA, the mandate to issue guidelines in this area[1] while Regulation (EU) 2023/1114 (MiCAR) sets out a specific mandate for the EBA in consultation with ESMA and ECB to develop guidelines on internal governance arrangements regarding issuers of asset-referenced tokens (ARTs). Directive 2014/65/EU (MiFID II) contains explicit provisions regarding the outsourcing to TPSPs of operational functions in the field of investment services and activities. Directive 2015/2366/EU (PSD2) sets out requirements for the outsourcing of operational functions by payment institutions. Outsourcing arrangements are considered as a subset of third-party arrangements. The entry into force of Regulation (EU) 2022/2554 (DORA) since January 2023 also needs to be taken into account, since information and communication technology (ICT) services provided by TPSP to financial entities are within DORA's scope of application. In this regard, all non-ICT related services provided by TPSP to financial entities are within the scope of these Guidelines. A close alignment for the management of third-party risk between both frameworks should be achieved to ensure a level playing field and foster supervisory convergence.

Each financial entity's management body remains responsible for its activities, at all times; to this end, the management body should ensure that sufficient and adequate resources are available to appropriately support and ensure the performance of those responsibilities, including managing and overseeing all risks including stemming from third-party arrangements in particular when they are used to provide critical or important functions. The use of TPSPs must not lead to a situation in which a financial entity becomes an 'empty shell' that lacks the substance to remain authorised.

With regard to TPSPs located in third countries, financial entities are expected to take particular care that compliance with EU legislation and regulatory requirements (e.g. professional secrecy, access to information, protection of personal data, data processing and storage) is ensured and that

[1] See Final Report on GL on internal governance under IFD (europa.eu).

the competent authority is able to effectively supervise financial entities, in particular regarding critical or important functions provided by TPSPs.

The Guidelines set out which arrangements with TPSPs are to be considered for a sound management of third-party risks and provide criteria for the identification of critical or important functions that have a material impact on the financial entity's risk profile. If such critical or important functions are performed by TPSPs, stricter requirements apply to these third-party arrangements than to other third-party arrangements.

Competent authorities are required to effectively supervise financial entities' third-party arrangements, including identifying and monitoring concentrations risk at individual TPSPs and assessing whether such concentrations could pose a risk to the stability of the financial system. To identify such concentrations risk, competent authorities should be able to rely on comprehensive documentation on third-party arrangements compiled by financial entities.

3. Background and rationale

1. Trust in the reliability of the financial system is crucial for its proper functioning and is a prerequisite if it is to contribute to the economy as a whole. Effective internal governance arrangements are fundamental for credit institutions subject to Directive 2013/36/EU[2] (CRD), investment firms that do not meet all the conditions to qualify as small and non-interconnected under Article 12(1) of Regulation (EU) 2019/2033[3] (IFR), issuers of asset-referenced tokens (ARTs) subject to Regulation (EU) 2023/1114[4] (MiCAR), payment institutions as defined in Article 4(4) of Directive (EU) 2015/2336[5] (PSD2), electronic money institutions within the meaning of Directive 2009/110/EC[6] (EMD) and creditors as defined in point (2) of Article 4 of Directive 2014/17/EU[7] (MCD) which are financial institutions (all together referred to as 'financial entities') and the financial system they form part of, to operate well.

2. Over recent years, there has been an increasing tendency by financial entities to rely on TPSPs to reduce costs, improve flexibility, efficiency including effectiveness of internal controls and to achieve economies of scale, e.g. by centralising functions within a group or institutional protection scheme. However, the use of TPSPs by financial entities is also one of the main drivers of operational risks. It is therefore necessary for financial entities to establish robust operational risk management and sound operational resilience capabilities.

3. The provision of important or critical functions or part thereof in particular by TPSPs located outside the EU creates specific risks both for financial entities and for their competent authorities and should be subject to appropriate oversight. Any third-party arrangements regarding non-information and communication technology (non-ICT) related services that would result in the delegation by the management body of its responsibility, altering the relationship and obligations of the financial entity towards its clients, undermining the conditions of its authorisation or removing or modifying any of the conditions subject to which the financial entity's authorisation was granted, should not be permitted. Third-party arrangements should not impair the quality and independence of the financial entity internal controls functions or the ability of those financial

[2] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

[3] Regulation (EU) 2019/2033 of the European Parliament and of the Council of 27 November 2019 on the prudential requirements of investment firms and amending Regulations (EU) No 1093/2010, (EU) No 575/2013, (EU) No 600/2014 and (EU) No 806/2014 (OJ L 314, 5.12.2019, p. 1–63).

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

[5] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[6] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

[7] Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ L 060, 28.2.2014, p. 34).

entities and the competent authorities to oversee and supervise compliance with legal and regulatory requirements.

4. The responsibility of the financial entity's management body and all its activities can never be delegated to TPSPs.

5. Third-party arrangements including outsourcing are also relevant in the context of gaining or maintaining access to the EU's financial system. Third-country financial entities may wish to set up subsidiaries or branches in the EU to get or maintain access to the EU's financial system and markets infrastructures. In this context, third-country financial entities may seek to minimise the transfer of the effective performance of business activities to their subsidiaries and branches located in the EU, e.g. by relying on the functions provided by the third-country parent entity or other third-country group entities.

6. The use of TPSPs must not lead to a situation where a financial entity becomes an 'empty shell' that lacks the substance to remain authorised. To this end, the management body should ensure that sufficient resources are available to appropriately support and ensure the performance of its responsibilities, including overseeing the risks and managing the third-party arrangements.

7. Functions that are considered critical under a resolution perspective may also be provided by TPSPs. Third-party arrangements should not create impediments to the resolvability of the financial entity where applicable.

8. Competent authorities must grant authorisation in full compliance with EU law; they should set a strict framework, in line with these Guidelines, on the use of TPSPs by financial entities in the EU to third-country entities; and should ensure consistent and effective supervision. Competent authorities should also ensure that financial entities have effective policies and procedures in place to comply with the relevant legal and regulatory frameworks at all times.

9. Financial entities should be able to effectively control and challenge the quality and performance of functions provided by TPSPs and be able to carry out their own risk assessment and ongoing monitoring. It is not sufficient for financial entities to undertake only formal assessments of whether functions provided by TPSPs meet regulatory requirements.

10. The Guidelines should be read in conjunction with, but without prejudice to, the EBA Guidelines on internal governance under CRD, the EBA Guidelines on internal governance under IFD, the EBA Guidelines on internal governance arrangements for issuers of ARTs under MiCAR, the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) under CRD, the requirements on organisational arrangements (such as, inter alia, outsourcing, internal control functions) provided in MiFID II and relevant delegated acts, and any guidance provided by ESMA for the provision of investment services and activities (such as, inter alia, the ESMA guidelines on compliance function[8]). For payment institutions, these Guidelines should be read in conjunction with the relevant EBA Guidelines mandated under Directive 2015/2366/EU (Payment Services Directive; PSD2).

[8] See Final Report Guidelines on certain aspects of the MiFID II compliance function requirements.

11. These Guidelines do not provide for any guidance with regard to the use of third-party arrangements in the context of the AML/CFT framework, since a specific mandate is foreseen under Article 18 of Regulation (EU) 2024/1624[9].

12. These Guidelines are subject to the principle of proportionality; they are to be applied in a manner that is appropriate, taking into account the financial entity size and internal organisation and the nature, scope and complexity of its activities.

Rationale and objective of the Guidelines

13. The EBA is updating the EBA Guidelines on outsourcing arrangements issued in 2019, which applied exclusively to credit institutions and investment firms subject to CRD, payment institutions and electronic money institutions, with the aim of establishing a more harmonised framework regarding the sound management of third-party risk and to take into account the entry into force of Regulation (EU) 2022/2554 (DORA). The scope of application of these Guidelines now covers institutions subject to Directive 2013/36/EU (CRD), investment firms that do not meet all the conditions to qualify as small and non-interconnected under Article 12(1) of Regulation (EU) 2019/2033 (IFR), payment and electronic money institutions (referred to as 'payment institutions'), issuers of ARTs subject to MICAR and creditors as defined in point (2) of Article 4 of Directive 2014/17/EU (MCD) which are financial institutions. The Guidelines are not directly addressed to credit intermediaries or to account information service providers that are only registered for the provision of service 8 of Annex I to the PSD2. The use of third-party arrangements between credit institutions, payment institutions, investment firms, and such entities are within the scope of the Guidelines when such entities act as TPSPs.

14. The Guidelines take into account and are consistent with the current requirements under the Directive 2013/36/EU (CRD), Directive 2014/65/EU[10] (MiFID II), Directive 2019/2034/EU[11] (IFD), Directive 2009/110/EC (Electronic Money Directive; EMD), Directive (EU) 2015/2366 (PSD2), Directive 2014/59/EU [12] (Bank Recovery and Resolution Directive; BRRD), Regulation (EU) 2022/2554 (DORA) and the respective delegated regulations adopted by the European Commission. In addition, international developments in this area, such as the work performed by the Financial Stability Board (FSB) and the Basel Committee on Banking Supervision (BCBS), have been taken into account.

[9] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L 2024/1624, 19.6.2024).

[10] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

[11] Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU.

[12] Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).

15. Under Article 16 of Regulation (EU) No 1093/2010[13] (the EBA Regulation), the EBA is required to issue Guidelines and recommendations addressed to competent authorities and financial institutions with a view to establish consistent, efficient and effective supervisory practices and to ensure the common, uniform and consistent application of EU law. In particular, the conditions for the management of third-party risk and the use of TPSPs for the provision of non-ICT related functions to financial entities are not harmonised to the same extent as for financial entities subject to DORA with regard to ICT services. A close alignment for the management of third-party risk between both frameworks should be made to ensure a level playing field and foster supervisory convergence.

16. Divergent regulatory approaches carry a risk of regulatory arbitrage, which may expose the EU to financial stability risks. Those risks are particularly acute in relation to the use of TPSPs located in third countries, where supervisory authorities may lack the necessary powers and tools to adequately and effectively supervise TPSPs that provide critical or important functions to EU financial entities.

17. To embrace all existing legislation and to ensure a level playing field for all financial entities within the scope of these Guidelines, the wording used under DORA/MiFID II/Solvency II is used within the Guidelines. It is necessary to provide a clear definition of what is considered a third-party arrangement, including outsourcing. The definition of 'critical or important function' provided in the Guidelines is in line with the one provided in Article 3(22) of DORA, but also with MiFID II and its related Commission Delegated Regulation (EU) 2017/565[14]. It should be noted that the definition of 'critical or important function' for the purpose of third-party risk management used in these Guidelines is different from the definition of 'critical functions' under Article 2(1)(35) of BRRD. However, the definition of 'critical or important function' in these Guidelines encompasses the 'critical functions' as defined in Article 2(1) point (35) of BRRD. The use of the term 'critical or important functions' is also further specified in Article 30 of the Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II. The same approach exists under Directive 2009/138/EC[15] (Solvency II), while, in the context of outsourcing, the PSD2 uses 'important function' for the purpose of identifying functions under outsourcing arrangements for which specific requirements apply.

18. Article 109(2) CRD requires that parent undertakings and subsidiaries subject to this Directive meet the governance requirements not only on an individual basis but also on a consolidated or sub-consolidated basis, unless waivers for the application on an individual basis have been granted under Article 21 CRD or Article 109(1) CRD in conjunction with Article 7 of Regulation (EU) No 575/2013[16] (Capital Requirements Regulation; CRR). It should be ensured that parent undertakings and subsidiaries subject to the CRD implement such arrangements, processes and mechanisms in their subsidiaries not subject to this Directive (e.g. payment institutions and

[13] 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).

[14] Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.

[15] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking up and pursuit of the business of Insurance and Reinsurance.

[16] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

electronic money institutions, issuers of ARTs, investment firms, as well as firms subject to Directive 2011/61/EU[17] and Directive 2009/65/EC[18]). Governance arrangements, processes and mechanisms must be consistent and well-integrated and those subsidiaries not subject to the CRD must also be able to produce any data and information relevant for the purpose of supervision.

Governance of third-party arrangements

19. Institutions, in accordance with Article 74 of CRD, payment institutions in line with Article 11 of PSD2, investment firms in accordance with Article 26 of IFD and issuers of ARTs in accordance with Article 34 of MiCAR should have robust internal governance arrangements that include a clear organisational structure. Third-party arrangements are one aspect of financial entities' organisational structure. The Guidelines include elements that aim to ensure that:

    a. there is effective day-to-day management by the management body in its management function and senior management;

    b. there is effective oversight by the management body in its supervisory function;

    c. there is a written policy on sound management of third-party risks and there are sound processes related to third-party risk management;

    d. financial entities have an effective internal control and risk management framework, including with regard to the management of third-party risk;

    e. all the risks associated with the provision of critical or important functions by TPSPs are identified, assessed, monitored, managed, reported and, as appropriate, mitigated;

    f. there are appropriate plans for the exit from third-party arrangements regarding critical or important functions, e.g. by migrating to another TPSP or by reintegrating the critical or important functions; and

    g. competent authorities remain able to effectively supervise financial entities, including the functions that have been provided by TPSPs.

20. Financial entities must define criteria or establish a methodology to determine whether the function to be provided by a TPSP is considered critical or important. In addition to the definition of "critical or important function", the Guidelines specify further criteria to ensure that the assessment of the criticality or importance of functions is more harmonised. The provision of critical and important functions by TPSPs can have a material impact on the financial entities' risk profile. To this end, additional requirements apply to the provision of critical or important functions by TPSP to financial entities, which aim to ensure the soundness of their governance arrangements and that competent authorities can exercise effective supervision.

21. The risks to be considered include those associated with the financial entities' relationship with the TPSP, the risks caused by allowing subcontracting, the concentration risk posed by multiple

[17] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010.

[18] Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS).

arrangements with the same TPSP and/or the concentration risk posed by the provision of critical or important functions by a limited number of TPSPs or with closely connected TPSPs. The concentration to a limited number of TPSPs is particularly relevant for competent authorities when supervising the impact of third-party arrangements on the stability of the financial system. In addition, overreliance on the provision of critical or important functions by TPSP is likely to impact the conditions for authorisation and to heighten both concentration risks and the risk of creating 'empty shells' that would lack the substance to remain authorised.

22. Similarly, third-party arrangements with long or complex operational chains or with a large number of parties involved are likely to result in additional challenges both for financial entities and for competent authorities.

23. Each form of third-party arrangement has its specific risks and advantages. Without prejudice to the waivers included in Article 21 CRD that may be granted when the conditions under Article 10 of CRR are met and waivers under Article 109(1) CRD that apply when the derogation under Article 7 CRR has been granted by competent authorities, intragroup third-party arrangements are subject to the same regulatory framework as third-party arrangements with TPSPs outside the group. Intragroup third-party arrangements are not necessarily less risky than third-party arrangements with TPSPs outside the group. In particular, with regard to intragroup third-party arrangements, financial entities need to take into account conflicts of interest that may be caused by third-party arrangements, e.g. between different entities within the scope of consolidation.

24. Where financial entities intend to use entities within the group to provide or support important or critical functions, they should ensure that the selection of a group entity is based on objective reasons and that the conditions of the arrangement are set at arm's length and explicitly deal with conflicts of interest that such an arrangement may entail. Financial entities should clearly identify all relevant risks and detail the mitigation measures and controls put in place to ensure that the third-party arrangements with affiliated entities do not impair the financial entity's ability to comply with the relevant legal and regulatory frameworks. However, when using a TPSP belonging to the same group, financial entities may have a higher level of control over the function provided by the intragroup TPSP, which they could take into account in their risk assessment.

25. The same aspects that are relevant for third-party arrangement within a group hold true when institutions that are members of an institutional protection scheme use a central service provider to provide functions.

26. The provision of critical or important functions by TPSPs located in third countries must be subject to additional safeguards that ensure that these third-party arrangements do not lead to an undue increase in risks or do not impair the ability of competent authorities to effectively supervise financial entities.

27. Financial entities should have in any case robust governance arrangements in place for third-party arrangements that are not considered critical or important. Therefore, the Guidelines provide for further specifications regarding all third-party arrangements taking into account the application of the proportionality principle.

28. Arrangements with TPSPs should not lower financial entities' obligation to comply with legal and regulatory requirements, and internal corporate values, e.g. those set out within a code of

conduct. When selecting TPSPs, financial entities should carefully pay attention to human rights and to ESG risks and take into account the impact of their third-party arrangements on all stakeholders. Such aspects are of particular relevance when TPSPs are located in third countries.

29. Financial entities should manage the contractual relationship; this includes evaluating and monitoring the ability of the TPSP to fulfil the conditions included in the written third-party agreements. Indeed, increased reliance on the TPSPs for the provision of functions, in particular with regard to critical or important functions, may have an impact on financial entities ability to manage their risks, such as operational risks, including compliance and reputational risks.

30. Specific guidance is provided on the relationship between financial entities and TPSPs, including on their rights and obligations. The Guidelines specify a set of aspects that should be included within each written third-party agreement.

31. Third-party arrangements also need to be considered in the context of institutions' recovery and resolution planning; the operational continuity of critical functions must be ensured even when in financial distress or during financial restructuring or resolution. A business decision to outsource a function should not in any way impede the resolvability of the institution.

32. The financial entities' and competent authorities', including resolution authorities, right to audit, inspections and access to information, accounts and premises should be ensured within each written third-party agreement. The right to audit is key for providing the appropriate assurance that at least critical or important functions provided by TPSPs, as well as functions that may become critical or important in the future, are provided as contractually agreed and in line with legal and regulatory requirements. To ensure that credit institutions can be effectively supervised, audit and access rights for competent authorities need to be ensured for all third-party arrangements. The same rights for competent authorities should be considered for all other financial entities. Further guidance is provided on how financial entities can exercise their audit rights in a risk-based manner, taking into account concerns regarding the organisational burden for both the financial entities and the TPSP, as well as practical, security and confidentiality concerns regarding physical access to certain types of business premises. Pooled audits performed by credit institutions are not to be considered as "third-party arrangements" as per the scope of these guidelines.

33. The third-party agreement should specify whether subcontracting of critical or important functions, or material parts thereof, is permitted. Hence, the Guidelines specify the conditions for the use of subcontracting by the financial entities in the case of critical or important functions provided by TPSPs; any function to be subcontracted and considered as critical or important should be recorded in the register. Financial entities should always have the right to terminate the contract if planned changes to functions, including such changes caused by subcontracting, would have an adverse effect on the functions provided.

Supervision and concentration risks

34. It is of particular importance that competent authorities have a comprehensive overview of third-party arrangements of financial entities, as this enables them to exercise their supervisory powers. Financial entities should therefore document all their third-party arrangements. In addition, financial entities should inform competent authorities or engage with competent authorities in a dialogue regarding planned and amended third-party arrangements with regard

to critical or important functions. The final responsibility for the arrangements with TPSPs always remains within the financial entities. To this end, the Guidelines set out specific documentation requirements for financial entities' third-party arrangements.

35. Competent authorities need to identify the concentration of third-party arrangements by TPSPs. The concentration of third-party arrangements with TPSPs and as regards critical or important functions may, if the provision of the service fails, lead to the disruption of the provision of financial services by multiple financial entities. If TPSPs fail or are no longer able to provide their services, including in the case of severe business disruption caused by external events, this may cause systemic risks to the financial system.

4. Draft Guidelines

EBA/GL/2025/xx

Dd Month yyyy

Guidelines on the sound management of third-party risk

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[19]. 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 out the EBA's 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 which the 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 financial institutions.

Reporting requirements

3. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA that they comply or intend to comply with these Guidelines, or otherwise give reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/XX/XX'. 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).

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

2. Subject matter, scope and definitions

Subject matter

5. These Guidelines specify the internal governance arrangements, including sound risk management that institutions, investment firms that do not meet all the conditions to qualify as small and non-interconnected under Article 12(1) of Regulation (EU) 2019/2033[20] (IFR), payment institutions, electronic money institutions, issuers of asset-referenced tokens (ARTs) and creditors as defined in point (2) of Article 4 of Directive 2014/17/EU[21] (MCD) which are financial institutions should implement when they rely on third-party service providers (TPSPs) to provide functions, in particular critical or important functions or part thereof.

6. The Guidelines specify how the arrangements referred to in the previous paragraph should be reviewed and monitored by competent authorities, in the context of Article 97 of Directive 2013/36/EU (CRD) on supervisory review and evaluation process (SREP), Article 36 of Directive 2019/2034/EU (IFD)[22], Article 9(3) of Directive (EU) 2015/2366 (PSD2), Article 5(5) of Directive 2009/110/EC[23] (EMD) and Article 35(3) of Regulation (EU) 2023/1114[24] (MiCAR) by fulfilling their duty to monitor the continuous compliance of entities to which these Guidelines are addressed with the conditions of their authorisation.

7. The management of information and communication technology (ICT) risk and the use of TPSPs to provide ICT services as defined in Article 3(21) of Regulation EU 2022/2554[25] (DORA) are not under the scope of application of these Guidelines as they fall under the scope of DORA. In this regard, these Guidelines only cover the use of TPSPs providing or supporting functions that are not qualified as ICT services under DORA. Consistency has been ensured, to the extent possible with DORA and its relevant mandates; while DORA provides for the framework on the management of third-party risks with regard to ICT services, those Guidelines apply for non-ICT related services provided by TPSPs.

[20] Regulation (EU) 2019/2033 of the European Parliament and of the Council of 27 November 2019 on the prudential requirements of investment firms and amending Regulations (EU) No 1093/2010, (EU) No 575/2013, (EU) No 600/2014 and (EU) No 806/2014 (OJ L 314, 5.12.2019, p. 1–63).

[22] Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU.

[23] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

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

[25] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1-79).

Addressees

8. These Guidelines are addressed to competent authorities as defined in points (i), (vi) and (viii) of Article 4(2) of Regulation (EU) No 1093/2010 and in Article 3(1), point (35)(a) of Regulation (EU) 2023/1114.

9. These Guidelines are also addressed to financial institutions as defined in Article 4(1) of Regulation No 1093/2010 that are institutions as defined in point (3) of Article 4(1) of Regulation (EU) No 575/2013 (CRR), third-country branches, as defined in point 1 of Article 47(3) of Directive 2013/36/EU[26], investment firms as defined in point (1) of Article 4(1) of Directive (EU) 2014/65 (MiFID II) with the exception of small and non-interconnected investment firms under Article 12(1) of Regulation (EU) 2019/2033, payment institutions as defined in Article 4(4) of Directive (EU) 2015/2336, electronic money institutions within the meaning of Directive 2009/110/EC, issuers of asset referenced tokens (ARTs) as defined in Article 3(1), point 10 of Regulation (EU) 2023/1114 and creditors as defined in point (2) of Article 4 of Directive 2014/17/EU[27] (MCD) which are financial institutions referred to in this paragraph. In line with Article 3(3) of Directive 2013/36/EU, these Guidelines are also addressed to financial holding companies and mixed financial holding companies that have been granted approval in accordance with Article 21a(1) of that Directive. For the purposes of these Guidelines, entities referred to in this paragraph should collectively be referred to as 'financial entities'.

10. Account information service providers that only provide the service in point 8 of Annex I of Directive (EU) 2015/2366 are not included in the scope of application of these Guidelines, in accordance with Article 33 of that Directive.

11. For the purpose of these Guidelines, any reference to 'payment institutions' includes 'electronic money institutions'.

Scope of application

12. Without prejudice to Directive 2014/65/EU[28] and Commissions Delegated Regulation (EU) 2017/565[29] which contain specific requirements regarding outsourcing by credit institutions and investment firms providing investment services and performing investment activities, as well as relevant guidance issued by the European Securities and Markets Authority regarding investment services and activities, institutions as defined in point 3 of Article 3(1) of Directive

[26] For EU branches of third country credit institutions, these guidelines should be read in conjunction with the EBA guidelines on internal governance under 2013/36/EU.

[27] Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ L 060, 28.2.2014, p. 34).

[28] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

[29] Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (OJ L 87, 31.3.2017, p. 1).

2013/36/EU, Class 1 minus[30] and Class 2[31] investment firms should comply with these Guidelines on an individual basis, sub-consolidated basis and consolidated basis, as relevant. The application on an individual basis might be waived by competent authorities under Article 21 of Directive 2013/36/EU or Article 109(1) of Directive 2013/36/EU in conjunction with Article 7 of Regulation (EU) No 575/2013. Institutions subject to Directive 2013/36/EU should comply with these Guidelines on a consolidated and sub-consolidated basis as set out in Article 21 and Articles 108 to 110 of Directive 2013/36/EU. Class 2 investment firms subject to Directive 2019/2034/EU should comply with these Guidelines on a consolidated basis in accordance with Article 25 of Directive (EU) 2019/2034.

13. Without prejudice to Article 8(3) of Directive (EU) 2015/2366 and Article 5(7) of Directive 2009/110/EC, payment institutions and electronic money institutions should comply with these Guidelines on an individual basis.

14. Issuers of ARTs which are not institutions subject to Directive 2013/36/EU should comply with these Guidelines on an individual basis and where applicable, on a group wide basis[32].

Definitions

15. Unless otherwise specified, terms used and defined in Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive 2019/2034/EU, Regulation (EU) 2019/2033, Directive 2009/110/EC, Directive (EU) 2015/2366, Regulation (EU) 2023/1114, the EBA Guidelines on internal governance under Directive 2013/36/EU[33], the EBA Guidelines on internal governance under Directive (EU) 2019/2034[34] and the EBA Guidelines on the minimum content of the governance arrangements for issuers of asset-referenced tokens under Regulation (EU) 2023/1114[35] have the same meaning in these Guidelines.

16. In addition, for the purposes of these guidelines, the following definitions apply:

Third-party arrangement	means an arrangement[36] of any form between a financial entity and a third-party service provider, including intragroup third-party service providers, for the provision of one or more functions to the financial entity.

[30] This category of investment firms refers to investment firms as defined in point (1) of Article 4(1) of Directive (EU) 2014/65 that are subject to Title VII of Directive 2013/36/EU in application of Article 1(2) and (5) of Regulation (EU) 2019/2033.

[31] This category of investment firms refers to investment firms that do not fall under Article 2(2) of Directive (EU) 2019/2034 and do not meet the conditions to qualify as small and non-interconnected investment firms under Article 12(1) of Regulation (EU) 2019/2033.

[32] See EBA Guidelines on on the minimum content of the governance arrangements for issuers of asset-referenced tokens under Regulation (EU) 2023/1114 (EU) (EBA/GL/2024/06).

[33] See: EBA Guidelines on internal governance under Directive 2013/36/EU.

[34] See: Final Report on GL on internal governance under IFD (europa.eu).

[35] See: Final report on draft Guidelines on internal governance of issuers of ARTs (europa.eu).

[36] The term excludes an arrangement between a third-party service provider and any entity in the supply chain (i.e. a subcontractor to the financial entity).

	This includes outsourcing arrangements as a subset.
Outsourcing arrangement	means an arrangement of any form between a financial entity and a third-party service provider, including intragroup third-party service providers by which the third-party service provider performs, on a recurrent or an ongoing basis, a function that would otherwise be undertaken by the financial entity itself.
Third-party risk	means a risk that may arise for a financial entity in relation to the use of function provided by third-party service providers or by subcontractors of the latter, including the provision of a function or the support to a function, including through outsourcing arrangements.
Function	means any process, service or activity or part of it.
Critical or important function[37]	means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.
Subcontracting	means a situation where a third-party service provider under an arrangement of any form further transfers a function to another service provider[38].
Third-party service provider	means an undertaking providing or supporting a function under an arrangement with a financial entity.
Intra-group third-party service provider	means an undertaking that is part of a financial group and that provides or supports functions to financial entities within the same group or to financial entities belonging to the same institutional protection scheme, including to their parent undertakings, subsidiaries or other entities that are under common ownership or control.

[37] The wording 'critical or important function' is used only for the purpose of these Guidelines and it is not related to the definition of 'critical functions' for the purpose of the recovery and resolution framework as defined under Article 2(1), point (35) of Directive 2014/59/EU (BRRD).

[38] For the assessment, the provisions in Section 3 apply; sub-contracting has also been referred to in other documents as a 'chain of subcontracting' or the use of nth party service providers.

Management body	means a financial entity's body or bodies, which are appointed in accordance with national law, which are empowered to set the financial entity's strategy, objectives and overall direction, and which oversee and monitor management decision-making and include the persons who effectively direct the business of the financial entity and the directors and persons responsible for the management of the payment institution or the electronic money institution.
Concentration risk	means an exposure to individual or multiple related third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of such provider may potentially endanger the ability of a financial entity to deliver critical or important functions or cause it to suffer other types of adverse effects, including large losses, or endanger the stability of the financial system.
Operational resilience	means the ability of a financial entity to deliver critical or important functions through disruption. This ability enables a financial entity either directly or indirectly, including through the use of functions provided by third-party service providers, to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical or important function through disruption.

3. Implementation

Date of application

17. These Guidelines apply from [date] to all third-party arrangements entered into, reviewed or amended on or after this date.

18. Financial entities should review and amend accordingly existing third-party arrangements with a view to ensuring that these are compliant with these Guidelines.

19. Where the review of third-party arrangements of critical or important functions is not finalised by [date: 2 years from the date of application], financial entities should inform their competent authority of that fact, including the measures planned to complete the review or the possible exit strategy.

Transitional provisions

20. Financial entities should complete the documentation of all existing third-party arrangements in line with these Guidelines following the first renewal date of each existing third-party arrangement, but by no later than [date: 2 years from the date of application].

Repeal

21. The EBA Guidelines on outsourcing of 25 February 2019 are repealed with effect from [date].

Question n. 1

Are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?

4. Guidelines on the sound management of third-party risks

Title I – Proportionality: group application and institutional protection schemes

1 Proportionality

22. Financial entities and competent authorities should, when complying or supervising compliance with these Guidelines, have regard to the principle of proportionality. The proportionality principle aims to ensure that governance arrangements, including those related to third-party risk management, are consistent with the individual risk profile, the nature and business model of the financial entity, and the scale and complexity of their activities so that the objectives of the regulatory requirements are effectively achieved.

23. When applying the requirements set out in these Guidelines, financial entities should take into account the complexity of the functions provided by TPSPs, the risks arising from the third-party arrangement, the criticality or importance of the function provided by TPSPs and the potential impact of such arrangement on the continuity of their activities.

24. When applying the principle of proportionality, financial entities[39] and competent authorities should take into account the criteria specified in Title I of the EBA Guidelines on internal governance under Directive 2013/36/EU, in Title I of the EBA Guidelines on internal governance under Directive (EU) 2019/2034, and Title I of the EBA Guidelines on the minimum content of the governance arrangements for issuers of asset-referenced tokens under Regulation (EU) 2023/1114.

2 Management of third-party risks by financial entities within groups and institutions that are members of an institutional protection scheme

25. In accordance with Article 109(2) of Directive 2013/36/EU, these Guidelines should also apply on a consolidated and sub-consolidated basis taking into account the prudential scope of consolidation[40]. For this purpose, the EU parent undertaking or the parent undertaking in a Member State should ensure that internal governance arrangements, processes and

[39] Payment institutions should also refer to the EBA Guidelines under PSD2 on the information to be provided for the authorisation of payment institutions and electronic money institutions and the registration of account information service providers, which are available on the EBA's website under the following link: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2.

[40] See Article 4(1) points (47) and (48) of Regulation (EU) No 575/2013 regarding the scope of consolidation.

mechanisms in their subsidiaries, including payment institutions, investment firms and issuers of ARTs are consistent, well integrated and adequate for the effective application of these Guidelines at all relevant levels.

26. Where applicable, financial entities, in accordance with paragraph 25, and institutions that, as members of an institutional protection scheme, use centrally provided governance arrangements should comply with the following:

    a. where those financial entities have third-party arrangements with TPSPs within the group or the institutional protection scheme[41], the management body of those financial entities retains, also for such third-party arrangements, full responsibility for compliance with all regulatory requirements and the effective application of these Guidelines;

    b. where those financial entities partially or fully rely for the operational tasks of internal control functions on a TPSP within the group or the institutional protection scheme, for the monitoring and auditing of third-party arrangements, financial entities should ensure that, also for these arrangements, those operational tasks are effectively performed, including through the receiving of appropriate reports.

27. In addition to paragraph 26, financial entities within a group for which no waivers have been granted on the basis of Article 109 of Directive 2013/36/EU and Article 7 of Regulation (EU) No 575/2013, institutions that are a central body or that are permanently affiliated to a central body for which no waivers have been granted on the basis of Article 21 of Directive 2013/36/EU, or institutions that are members of an institutional protection scheme should take into account the following:

    a. where the operational monitoring of third-party arrangement is centralised (e.g. as part of a master agreement for the monitoring of third-party arrangements), financial entities should ensure that, at least for critical or important functions provided by TPSPs, both independent monitoring of the TPSP and appropriate oversight by each financial entity is performed, including by receiving, at least annually and upon request from such centralised function, reports that include, at least, the risk assessment and performance monitoring. In addition, financial entities should receive from the centralised function a summary of the relevant audit reports for critical or important functions provided by TPSPs and, upon request, the full audit report;

    b. financial entities should ensure that their management body will be duly informed of relevant planned changes regarding TPSPs that are monitored centrally and the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, including legal risks, compliance with

[41] In accordance with Article 113(7) CRR, institutional protection scheme means a contractual or statutory liability arrangement which protects those institutions that are a member of the scheme and in particular ensures their liquidity and solvency to avoid bankruptcy where necessary.

regulatory requirements and the impact on service levels, in order for them to assess the impact of these changes;

c. where those financial entities within the group, institutions affiliated to a central body or institutions that are part of an institutional protection scheme rely on a central pre-contractual analysis of the third-party arrangements, referred to in Section 12, each financial entity should receive a summary of the assessment and ensure that it takes into consideration its specific structure and risks within the decision-making process;

d. where the register of all existing third-party arrangements, as referred to in Section 10, is established and maintained centrally within a group or institutional protection scheme, competent authorities and all financial entities should be able to obtain their individual register without undue delay. This register should include all third-party arrangements, including third-party arrangements with TPSPs inside that group or institutional protection scheme;

e. where those financial entities rely on an exit plan, as referred to in Section 14, for a critical or important function that has been established at group level, within the institutional protection scheme or by the central body, all financial entities should receive a summary of the plan and be satisfied that the plan can be effectively executed.

28. Where waivers have been granted pursuant to Article 21 of Directive 2013/36/EU or Article 109(1) of Directive 2013/36/EU in conjunction with Article 7 of Regulation (EU) No 575/2013, the provisions of these Guidelines should be applied by the parent undertaking in a Member State for itself and its subsidiaries or by the central body and its affiliates as a whole.

29. Financial entities that are subsidiaries of an EU parent undertaking or of a parent undertaking in a Member State to which no waivers have been granted based on Article 21 of Directive 2013/36/EU or Article 109(1) of Directive 2013/36/EU in conjunction with Article 7 of Regulation (EU) No 575/2013 should ensure that they comply with these Guidelines on an individual basis.

Title II – Assessment of third-party arrangements

3 Sound management of third-party risks

30. Financial entities should establish whether an arrangement with a TPSP falls under the definition of third-party arrangement provided in these Guidelines. Within this assessment, consideration should be given to whether the function is provided or planned to be provided by a TPSP at least on a recurrent or ongoing basis. Consideration should also be given to whether the arrangement consists of a mere purchase of a good (e.g. plastic cards, card readers, office supplies, personal computers, furniture), which is excluded from the definition of third-party arrangement provided in these Guidelines.

31. Where an arrangement with a TPSP covers multiple functions[42], financial entities should consider all aspects of the arrangement within their assessment, e.g. if the third-party service provided includes the provision of operational task of risk management and prudential reporting both aspects should be considered together.

32. As a general principle, the following functions are excluded from the scope of these Guidelines[43]:

    a. a function that is legally required to be performed by a TPSP (e.g. statutory audit);

    b. global network infrastructures (e.g. Visa, MasterCard);

    c. clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members;

    d. global financial messaging infrastructures that are subject to oversight by relevant authorities (e.g. SWIFT);

    e. correspondent banking services;

    f. the acquisition of services that do not have material impact on the financial entities' risks exposures or on their operational resilience (e.g. advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's or payment institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators); and

    g. the acquisition of utilities already subject to a regulated framework (e.g. electricity, gas, water, telephone line).

4 Critical or important functions

33. Considering the risk assessment foreseen under Section 11.2, financial entities should always consider a function as critical or important in the following situations[44], where its disruption, discontinuity, defect or failure in its performance would materially impair:

[42] In case where for the provision of a non-ICT service, the arrangement with a third-party service provider also implies the use of ICT services as defined under Article 3(21) of DORA, it belongs to the financial entity to determine whether the use of ICT service is material for the provision of the services under the third-party arrangement and therefore triggers the application of DORA framework in lieu of the present Guidelines. See also ESAs Q&A DORA030.

[43] These exclusions are not intended to imply that financial entities should not take appropriate steps to manage risk of these arrangements.

[44] See also Article 30 Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive on the scope of critical and important operational functions in the context of the provision of investment services and activities.

a. their continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law;

b. their financial performance;

c. the soundness or continuity of their services and activities.

34. When relying on a TPSP for operational tasks of internal control functions, financial entities should always consider such tasks as critical or important functions, unless the assessment establishes that a failure to provide the tasks or the inappropriate provision of the tasks would not have an adverse impact on the effectiveness of the internal control functions.

35. When financial entities intend to use TPSPs for the provision of functions of banking activities or payment services or issuance of ARTs as defined in Article 3(1), point (6), of Regulation (EU) 2023/1114 to an extent that would require authorisation[45] by a competent authority, they should automatically consider such function as critical or important, as referred to in Section 12.1.

36. In the case of financial entities that are subject to Directive 2014/59/EU[46], particular attention should be given to the assessment of the criticality or importance of functions if the third-party arrangement concerns functions related to critical functions and core business lines as defined in Article 2(1), point (35) and 2(1), point (36) of Directive 2014/59/EU and using the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778[47]. Functions that are necessary to perform activities of core business lines or critical functions should be considered as critical or important functions for the purpose of these Guidelines, unless the financial entity's assessment establishes that a failure to provide the function or the inappropriate provision of such function would not have an adverse impact on the operational continuity of the core business line or critical function.

37. A function performed by financial entities should be considered critical or important taking into account at least the following factors:

a. whether the arrangement with TPSPs is directly connected to the provision of banking and investment services activities or payment services or issuance of ARTs[48] for which they are authorised;

[45] See the activities listed in Annex I of Directive 2013/36/EU.

[46] Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (BRRD) (OJ L 173, 12.6.2014, p. 190).

[47] Commission Delegated Regulation (EU) 2016/778 of 2 February 2016 supplementing Directive 2014/59/EU of the European Parliament and of the Council with regard to the circumstances and conditions under which the payment of extraordinary ex post contributions may be partially or entirely deferred, and on the criteria for the determination of the activities, services and operations with regard to critical functions, and for the determination of the business lines and associated services with regard to core business lines (OJ L 131, 20.5.2016, p. 41).

[48] See the activities listed in Annex I of Directive 2013/36/EU.

b. the potential impact of any disruption to the function provided by TPSPs or failure of TPSPs to provide the service at the agreed service levels on a continuous basis on their:

   i. short- and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;

   ii. business continuity and operational resilience;

   iii. operational risk and legal risks;

   iv. reputational risks;

   v. all other relevant risks, including credit risk, market risk, ESG risk and AML/CFT risk;

   vi. where applicable, recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation.

Question n. 2

Is Title II appropriate and sufficiently clear?

Title III – Governance framework

5 Sound governance arrangements and third-party risk

38. The management body of financial entities should define, approve and regularly review a strategy on the sound management of third-party risks. Such strategy should include the policy on the sound management of third-party risks as referred to in Section 6 and should apply on an individual basis and, where applicable, on a sub-consolidated and consolidated basis. The management body should, on the basis of an assessment of the overall risk profile of the financial entity and taking into account the application of proportionality, regularly review the risks identified in respect to third-party arrangements on the use of services supporting critical or important functions.

39. As part of the overall internal control framework[49], including internal control mechanisms[50], financial entities should have a holistic institution-wide risk management framework extending across all business lines and internal units. Under that framework, financial entities should identify and manage all their risks, including risks caused by arrangements with TPSPs. The risk management framework should also enable financial entities to make well-informed decisions on risk-taking and ensure that risk management measures are appropriately

[49] Financial entities under the scope of CRD should also refer to Title V of the EBA Guidelines on internal governance, whereas investment firms should refer to Title V of the EBA Guidelines on internal governance under Directive (EU) 2019/2034 and issuers of ARTs to Article 34 of MiCAR.

[50] Please also refer to Article 11 of Directive 2015/2366 (PSD2).

implemented, including with regard to ICT and cyber risks in accordance with Regulation (EU) 2022/2554 (DORA).

40. Financial entities, taking into account the principle of proportionality in line with Section 1, should identify, assess, monitor and manage all risks resulting from arrangements TPSPs to which they are or might be exposed. The risks, in particular the operational risks, of all arrangements with TPSPs, including the ones referred to in paragraph 30, should be assessed in line with Section 11.2.

41. Financial entities should ensure that they comply with all requirements under Regulation (EU) 2016/679, including for their third-party arrangements.

42. The use of TPSPs for the provision of functions cannot result in the delegation of the management body's responsibilities. Financial entities remain fully responsible and accountable for complying with all of their regulatory obligations, including the ability to oversee the use of TPSPs for the provision of critical or important functions.

43. The management body is at all times fully responsible and accountable for at least:

    a. ensuring that the financial entity meets on an ongoing basis the conditions with which it must comply to remain authorised, including any conditions imposed by the competent authority;

    b. the internal organisation of the financial entity;

    c. the identification, assessment and management of conflicts of interest;

    d. the setting of the financial entity's strategies and policies (e.g. the business model, the risk appetite, the risk management framework);

    e. overseeing the day-to-day management of the financial entity, including the management of all risks associated with third-party arrangements;

    f. the oversight role of the management body in its supervisory function, including overseeing and monitoring management decision-making;

    g. approving, overseeing and periodically reviewing the implementation of the business continuity policy regarding third-party arrangements;

    h. approving and periodically reviewing the internal audit plans, audits and material modifications to them regarding third-party arrangements.

44. The use of TPSPs should not lower the suitability requirements applied to the members of the management body of financial entities, senior management including key function holders, and persons responsible for the management of the payment institution. Financial entities

should have adequate competence and sufficient and appropriately skilled resources to ensure appropriate management and monitoring of third-party arrangements.

45. Financial entities should:

    a. clearly assign the responsibilities for the documentation, management and monitoring of third-party arrangements;

    b. allocate sufficient resources to ensure compliance with all legal and regulatory requirements, including these Guidelines and the documentation and monitoring of all third-party arrangements;

    c. taking into account Section 1 of these Guidelines, establish a role in order to monitor all third-party arrangements or designate a member of senior management within the financial entity as directly accountable to the management body and responsible for overseeing the third-party risks as part of the financial entity's internal control framework and the documentation of third-party arrangements[51]. Less complex financial entities should at least ensure a clear division of tasks and responsibilities for the management and control of third-party risks and may assign the role to a member of the financial entity's management body.

46. Financial entities should maintain at all times sufficient substance and not become 'empty shells' or 'letter-box entities'. To this end, they should:

    a. meet all the conditions of their authorisation[52] at all times, including the management body effectively carrying out its responsibilities as set out in paragraph 36 of these Guidelines;

    b. retain a clear and transparent organisational framework and structure that enables them to ensure compliance with legal and regulatory requirements including the ability to be audited and supervised;

    c. where operational tasks of internal control functions are provided by TPSPs (e.g. in the case of intragroup outsourcing or outsourcing within institutional protection schemes), exercise appropriate oversight and be able to manage the risks that are generated by the performance of critical or important functions by a TPSP; and

[51] This role can be combined with the one in charge of monitoring the arrangements concluded with ICT third-party service providers on the use of ICT services under Article 5(3) of DORA.

[52] See also the regulatory technical standards (RTS) under Article 8(2) of Directive 2013/36/EU on the information to be provided for the authorisation of credit institutions, and the implementing technical standards (ITS) under Article 8(3) Directive 2013/36/EU on standard forms, templates and procedures for the provision of the information required for the authorisation of credit institutions (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

For payment institutions, please refer to the EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and electronic money institutions and for the registration of account information service providers (Guidelines on authorisation and registration under PSD2).

d. have sufficient knowledge, resources and capacities to ensure compliance with points (a) to (c).

47. When using a TPSP, financial entities should at least ensure that:

a. they can take and implement decisions related to their business activities and critical or important functions, including with regard to those that have been provided by the TPSP;

b. they maintain the orderliness of the conduct of their business and the banking, investment and payment services they provide;

c. the risks related to current and planned third-party arrangements are adequately identified, assessed, managed and mitigated;

d. appropriate confidentiality arrangements are in place regarding data and other information;

e. an appropriate flow of relevant information with the TPSPs maintained;

f. with regard to the critical or important functions provided by the TPSP, they are able to undertake at least one of the following actions, within an appropriate time frame:

i. transfer the function to alternative TPSPs;

ii. reintegrate the function; or

iii. discontinue the business activities that are depending on the function.

g. where personal data are processed by service providers located in the EU and/or third countries, appropriate measures are implemented and data are processed in accordance with Regulation (EU) 2016/679.

6 Policy on third-party risk management

48. The management body of a financial entity[53] that has third-party arrangements in place or plans on entering into such arrangements should approve, regularly review, at least once a year, a written policy on third-party risk management and update it, as appropriate. The management body should also ensure its implementation, as applicable, on an individual, sub-consolidated and consolidated basis.

[53] See also the EBA Guidelines on the security measures for operational and security risks of payment services under PSD2, available under: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2.

49. The policy should include all the phases of the life cycle of third-party arrangements and define the principles, responsibilities and processes in relation to third-party arrangements. In particular, the policy should cover at least:

    a. the responsibilities of the management body in line with paragraphs 43, including its involvement, as appropriate, in the decision-making on the use of TPSPs for critical or important functions;

    b. the ultimate responsibility of financial entities to ensure that they comply with all applicable legal and regulatory requirements when they make use of third-party arrangements;

    c. the involvement of business lines, internal control functions and other individuals in respect of third-party arrangements;

    d. the identification of the role or member of senior management responsible for monitoring third-party arrangements, specifying how that role or member of senior management shall cooperate with the internal control functions, unless it is part of it, and setting out the reporting lines to the management body, including the nature of the information to report and the documents to provide, and the frequency of such reporting;

    e. the planning of third-party arrangements, including:

        i. establishing whether an arrangement with a TPSP could potentially fall under the definition of third-party arrangement provided in these Guidelines;

        ii. the definition of business requirements regarding third-party arrangements;

        iii. the criteria, including those referred to in Section 4, and processes for identifying critical or important functions;

        iv. risk identification, assessment and management in accordance with Section 11.2;

        v. due diligence checks on prospective TPSPs, including the measures required under Section 11.3;

        vi. procedures for the identification, assessment, management and mitigation of potential conflicts of interest, in accordance with Section 7;

        vii. business continuity planning in accordance with Section 8;

        viii. the approval process of new third-party arrangements;

    f. the implementation, monitoring and management of third-party arrangements, including:

i. the monitoring of the TPSP's performance in line with Section 13;

ii. the procedures for being notified and responding to changes to a third-party arrangement or TPSP (e.g. to its financial position, organisational or ownership structures, subcontracting);

iii. the independent review and audit of compliance with legal and regulatory requirements and policies;

iv. their renewal processes;

g. the documentation and record-keeping, taking into account the guidelines in Section 10;

h. the exit strategies and termination processes, including a requirement for a documented exit plan for each critical or important function to be provided by TPSPs where such an exit is considered possible taking into account possible service interruptions or the unexpected termination of a third-party arrangement.

50. The policy on third-party risk management should differentiate between the following:

a. ICT services, for which DORA requirements apply, and non-ICT services;

b. third-party arrangements on critical or important functions and those that are not;

c. functions provided by TPSPs that are authorised by a competent authority and those that are not;

d. intragroup third-party arrangements, third-party arrangements within the same institutional protection scheme (including entities fully owned individually or collectively by institutions within the institutional protection scheme) and the use of TPSPs outside the group; and

e. the use of TPSPs located within a Member State and third countries.

51. Financial entities should ensure that the policy on third-party risk management covers the identification of the following potential effects of critical or important functions provided by TPSPs and that these are taken into account in the decision-making process:

a. the financial entity's risk profile;

b. the ability to oversee the TPSP and to manage the risks;

c. the business continuity measures; and

d. the performance of their business activities.

7 Conflicts of interests

52. Financial entities[54] should identify, assess and manage conflicts of interests with regard to their third-party arrangements.

53. Where third-party arrangements create material conflicts of interest, including between entities within the same group or institutional protection scheme, financial entities need to take appropriate measures to manage those conflicts of interest.

54. When functions are provided by a TPSP that is part of a group or a member of an institutional protection scheme or that is owned by the financial entity, group or institutions that are members of an institutional protection scheme, the conditions, including financial conditions, for the service provided by TPSPs should be set at arm's length. However, within the pricing of services synergies resulting from providing the same or similar services to several institutions within a group or an institutional protection scheme may be factored in, as long as the TPSP remains viable on a stand-alone basis; within a group this should be irrespective of the failure of any other group entity.

8 Business continuity plans

55. Financial entities[55], should have in place, maintain and periodically test appropriate business continuity plans with regard to critical or important functions provided by TPSPs. The TPSP should also be involved in those tests as appropriate. Financial entities within a group or institutional protection scheme may rely on centrally established and periodically tested business continuity plans regarding their functions provided by TPSPs, in accordance with Section 2.

56. Business continuity plans should take into account the possible event that the quality of the provision of the critical or important function provided by a TPSP deteriorates to an unacceptable level or fails.

57. Such plans should also take into account the potential impact of the insolvency or other failures of TPSPs and, where relevant, political risks in the TPSP's jurisdiction.

58. Financial entities shall have their business continuity plans in line with the EBA Guidelines on internal governance under Directive 2013/36/EU[56], the EBA Guidelines on internal governance

[54] Financial entities within the scope of CRD should also refer to Title IV, Section 11, of the EBA Guidelines on internal governance while investment firms should refer to Section 10 of the EBA Guidelines on internal governance under Directive (EU) 2019/2034, and issuers of ARTs to the EBA RTS on conflict of interests under Article 32(5) of Regulation (EU) 2023/1114.

[55] Financial entities within the scope of CRD should also refer to the requirements under Article 85(2) of Directive 2013/36/EU and Title VI of the EBA Guidelines on internal governance while investment firms should refer to Title VI of the EBA Guidelines on internal governance under Directive (EU) 2019/2034, and issuers of ARTs to Title VI of the EBA Guidelines on the minimum content of the governance arrangements for issuers of asset-referenced tokens under Regulation (EU) 2023/1114].

[56] See: EBA Guidelines on internal governance (update ongoing).

under IFD (EBA/GL/2021/14) and the EBA GLs on the minimum content of the governance arrangements for issuers of ARTs.

9 Internal audit function

59. The activities of the internal audit function[57], where established, or the internal audit review should cover, following a risk-based approach, the independent review of functions provided by TPSPs. The audit plan[58] and programme should include, in particular, the third-party arrangements of critical or important functions. With regard to the third-party arrangement process, the internal audit review should at least ascertain:

    a. that the financial entity's framework for third-party arrangements, including the policy on third-party risk management, is correctly and effectively implemented and is in line with the applicable laws and regulation, the risk strategy and the decisions of the management body;

    b. the adequacy, quality and effectiveness of the assessment of the criticality or importance of functions;

    c. the adequacy, quality and effectiveness of the risk assessment for third-party arrangements and that the risks remain in line with the financial entity's risk strategy;

    d. the appropriate involvement of governance bodies; and

    e. the appropriate monitoring and management of third-party arrangements.

60. Financial entities should establish a formal follow-up process regarding internal audit findings, including for the timely verification and remediation of material audit findings which may have an impact risk on the proper execution of any third-party arrangements.

10 Documentation requirements

61. As part of their risk management framework, financial entities should maintain an updated register of information on all third-party arrangements at individual and, where applicable, at sub-consolidated and consolidated levels, as set out in Section 2, and should appropriately document all current third-party arrangements, distinguishing between arrangements for the provision of critical or important functions and other third-party arrangements. Financial

[57] Regarding the responsibilities of the internal audit function, institutions should refer to Section 22 of the EBA Guidelines on internal governance (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-), investment firms should refer to Section 20 of the EBA Guidelines on internal governance under Directive (EU) 2019/2034, issuers of ARTs to Section 16 of the EBA Guidelines on the minimum content of the governance arrangements for issuers of asset-referenced tokens under Regulation (EU) 2023/1114] and payment institutions should refer to Guideline 5 of the EBA guidelines on the authorisation of payment institutions and e-money institutions under PSD2 (Guidelines on authorisation and registration under PSD2).

[58] See also EBA Guidelines on the supervisory review and evaluation process: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing.

entities should maintain the documentation of ended third-party arrangements within the register and the supporting documentation for an appropriate period of at least 5 years.

62. Taking into account Title I of these Guidelines, and under the conditions set out in paragraph 27(d), for financial entities within a group, institutions permanently affiliated to a central body or financial entities that are members of the same institutional protection scheme, the register may be kept centrally and collected at the highest level of consolidation.

63. Taking into the application of the proportionality under Title I of the guidelines, the register shall be consistent to the extent possible, when not merged, with the register of information under Article 28(3) DORA, and financial entities are encouraged to avoid any discrepancies between those two registers. The register should include at least the following information for all existing third-party arrangements:

    a. a reference number for each third-party arrangement and the type of contractual arrangement chosen ("Standalone arrangement", "Overarching arrangement", or "Subsequent or associated arrangement"; for the latter option, the reference number of the overarching arrangement should be specified);

    b. the start date and, as applicable, the next contract renewal date, the end date including the reason of the termination or ending of the contractual arrangement and/or notice periods for the TPSP and for the financial entity;

    c. where applicable, the financial entities within the scope of the prudential consolidation or institutional protection scheme, that make use of the TPSPs;

    d. whether or not the TPSP or subcontractor is part of the group or a member of the institutional protection scheme or is owned by financial entities within the group or is owned by members of an institutional protection scheme;

    e. a brief description of the functions provided by the TPSPs;

    f. a category assigned by the financial entity that reflects the nature of the functions covered by the third-party arrangement as described where available, in Annex I, which should facilitate the identification of different types of arrangements; if the category is not available under Annex I, the financial entity should provide its own internal categorisation. If an arrangement covers multiple functions, then the financial entity should report as many categories as the functions provided;

    g. the name of the TPSP, an identifier (LEI, EUID for legal persons, alternative codes – eg. VAT number, Passport Number, National Identity Number - for individuals acting in a business capacity), the corporate registration number, the registered address and other relevant contact details, and the name of its ultimate parent company and an identifier (LEI, EUID) (if any);

h. the country or countries where the function is to be performed and where the data is processed including storage;

i. whether or not (yes/no) the function provided by a TPSP is considered critical or important, including, where applicable, a brief summary of the reasons why this function is considered critical or important;

j. the date of the most recent assessment of the criticality or importance of the function;

k. the total annual expense or estimated cost of each direct TPSP.

64. For the critical or important functions of third-party arrangements, the register should include at least the following additional information:

a. the governing law of the third-party arrangement;

b. the dates of the most recent audits;

c. where applicable, the names of any subcontractors to which material parts of a critical or important function are sub-contracted, including the country where the subcontractors are registered, an identifier (LEI, EUID for legal persons, alternative codes – eg. VAT number, Passport Number, National Identity Number - for individuals acting in a business capacity), the type of functions or material part subcontracted, the rank in the chain, the location from where the service is performed;

d. the outcome and date of the last assessment performed of the TPSP's substitutability (as easy, medium, highly complex or impossible to substitute);

e. the summary and date of the last assessment performed of the possibility of reintegrating a critical or important function into the financial entity or the impact of discontinuing the critical or important function together with the recovery time objective of the function and the recovery point objective of the function;

f. the existence of an exit plan from the TPSP ('Yes' or 'No');

g. identification of alternative TPSPs in line with paragraph 63 point (g);

h. the estimated annual budget cost of the third-party arrangement for the past year, together with the currency.

65. Financial entities should, upon request, make available to the competent authority either the full register of all existing third-party arrangements[59] or sections specified thereof, such as information on all third-party arrangements falling under one of the categories referred to in

[59] Please also refer to the EBA Guidelines on supervisory review and evaluation process, available under: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

Annex I of these Guidelines. Financial entities should provide this information in a processable electronic form (e.g. a commonly used database format, comma separated values).

66. Financial entities should, upon request, make available to the competent authority all information necessary to enable the competent authority to execute the effective supervision of the financial entity, including, where required, a copy of any third-party arrangement.

67. Financial entities [60], including payment institutions for the purpose of complying with Article 19(6) of Directive (EU) 2015/2366, should inform competent authorities in a timely manner and, where appropriate, engage in a supervisory dialogue with the competent authorities about any planned contractual arrangement on the provision of critical or important functions by TPSPs as well as when a function performed by a TPSP has become critical or important and provide at least the information specified in paragraphs 63 and 64.

68. Financial entities should inform competent authorities in a timely manner of material changes and/or severe events regarding their third-party arrangements that could have a material impact on the continuing provision of the financial entities' business activities.

69. Financial entities should appropriately document the assessments made under Title IV and the results of their ongoing monitoring (e.g. level of performance of the TPSP, compliance with agreed service levels, other contractual and regulatory requirements, updates to the risk assessment).

Question n. 3

Are Sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?

Title IV – Third-party arrangement process

11 Pre-contractual analysis

70. Before entering into any third-party arrangement, financial entities should:

    a. assess whether the third-party arrangement concerns a critical or important function, as set out in Title II;

    b. assess whether the supervisory conditions for contracting with TPSPs set out in Section 11.1 are met;

    c. identify and assess all of the relevant risks in relation to the third-party arrangement in accordance with Section 11.2;

    d. undertake appropriate due diligence on the prospective TPSP in accordance with Section 11.3;

e. identify and assess conflicts of interest that the use of TPSPs may cause in line with Section 7.

11.1 Supervisory conditions for contracting with third-party service providers

71. Financial entities should ensure that the use of TPSPs to provide functions of banking activities[61] or payment services, issuance of ARTs as defined in Article 3(1), point (6), of Regulation (EU) 2023/1114 or investment services as defined in Article 4, point (2) of Directive 2014/65/EU to an extent that the performance of that function requires authorisation or registration by a competent authority in the Member State where they are authorised, to a TPSP located in the same or another Member State takes place only if one of the following conditions is met:

    a. the TPSP is authorised or registered by a competent authority to perform such activities or services; or

    b. the TPSP is otherwise allowed to carry out those activities or services in accordance with the relevant national legal framework.

72. Without prejudice of the requirements established under Article 32 of the Commission Delegated Regulation (EU) 2017/565/EU, financial entities should ensure that the use of TPSPs for the provision of functions of banking activities or payment services or issuance of ARTs as defined in Article 3(1), point (6), of Regulation (EU) 2023/1114, or investment services as defined in Article 4, point (2) of Directive 2014/65/EU to an extent that the performance of that function requires authorisation or registration by a competent authority in the Member State where they are authorised, to a TPSP located in a third country takes place only if the following conditions are met:

    a. the TPSP is authorised or registered to provide that activity or service in the third country and is supervised by a relevant competent authority in that third country (referred to as a 'supervisory authority');

    b. there is an appropriate cooperation agreement, e.g. in the form of a memorandum of understanding or college agreement, between the competent authorities responsible for the supervision of the financial entity and the supervisory authorities responsible for the supervision of the TPSP; and

    c. the cooperation agreement referred to in point (b) should ensure that the competent authorities are able, at least, to:

[61] See Article 9 CRD with regard to the prohibition of persons or undertakings other than credit institutions from carrying out the business of taking deposits or other repayable funds from the public.

i. obtain, upon request, the information necessary to carry out their supervisory tasks pursuant to Directive 2013/36/EU, Directive (EU) 2015/2366, Directive 2009/110/EC, Directive 2014/65/EU, Directive 2019/2034/EU and Regulation (EU) 2023/1114;

ii. obtain appropriate access to any data, documents, premises or personnel in the third country that are relevant for the performance of their supervisory powers;

iii. receive, as soon as possible, information from the supervisory authority in the third country for investigating apparent breaches of the requirements of Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive (EU) 2015/2366, Directive 2009/110/EC, Directive 2014/65/EU, Directive 2019/2034/EU and Regulation (EU) 2023/1114; and

iv. cooperate with the relevant supervisory authorities in the third country on enforcement in the case of a breach of the applicable regulatory requirements and national law in the Member State. Cooperation should include, but not necessarily be limited to, receiving information on potential breaches of the applicable regulatory requirements from the supervisory authorities in the third country as soon as is practicable.

11.2 Risk assessment of third-party arrangements

73. Financial entities should assess the potential impact of third-party arrangements on all their relevant risks including the operational risk, the reputational risk, the legal risk and the concentration risk at entity level. They should take into account the assessment results when deciding whether the function should be performed by a TPSP and should take appropriate steps to avoid undue additional operational risks before entering into third-party arrangements.

74. Financial entities should assess:

    a. the potential impact of a third-party arrangement on their ability to:

        i. identify, monitor and manage all risks;

        ii. comply with all legal and regulatory requirements;

        iii. conduct appropriate audits regarding the function provided by TPSPs;

    b. the potential impact on the services provided to their clients;

    c. the size and complexity of any business area affected;

d. the possibility that a proposed third-party arrangement might be scaled up without replacing or revising an underlying agreement;

e. the ability to transfer a proposed third-party arrangement to another TPSP, if necessary or desirable, both contractually and in practice, including the estimated risks, impediments to business continuity, costs and time frame for doing so ('substitutability');

f. the ability to reintegrate the function provided by TPSPs into the financial entity, if feasible, necessary or desirable;

g. the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the financial entity and its clients, including but not limited to compliance with Regulation (EU) 2016/679[62].

75. The assessment should include, where appropriate, scenarios of possible risk events, including high-severity operational risk events. Within the scenario analysis, financial entities should assess the potential impact of failed or inadequate services, including the risks caused by processes, systems, people or external events. Financial entities, taking into account the principle of proportionality referred to in Section 1, should document the analysis performed and their results and should estimate the extent to which the arrangement would increase or decrease their risk level. Taking into account Title I, less complex financial entities may use qualitative risk assessment approaches, while large or complex financial entities should have a more sophisticated approach, including, where available, the use of internal and external loss data to inform the scenario analysis.

76. Within the risk assessment, financial entities should also take into account the expected benefits and costs of the proposed third-party arrangement, including weighting any risks that may be reduced or better managed against any risks that may arise as a result of such proposed arrangement, taking into account at least:

a. concentration risks at entity level, including from:

i. using a TPSP that is not easily substitutable; and

ii. multiple third-party arrangements with the same TPSP or closely connected TPSPs;

b. the aggregated risks resulting from the use of TPSPs to perform several functions across the financial entity and, in the case of groups of institutions or institutional protection schemes, the aggregated risks on a consolidated basis or on the basis of the institutional protection scheme;

[62] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

c. in the case of significant institutions, the step-in risk, i.e. the risk that may result from the need to provide financial support to a TPSP in distress or to take over its business operations; and

d. the measures implemented by the financial entity and by the TPSP to manage and mitigate the risks.

77. Where the third-party arrangement includes the possibility that the TPSP subcontracts critical or important functions to subcontractors, financial entities should take into account:

a. the risks associated with subcontracting, including the additional risks that may arise if the subcontractor is located in a third country or a different country from the TPSP; and

b. the risk that long and complex chains of subcontracting reduce the ability of financial entities to oversee the critical or important function and the ability of competent authorities to effectively supervise them.

78. When carrying out the risk assessment prior to the conclusion of the third-party arrangement and during ongoing monitoring of the TPSP's performance, financial entities should, at least:

a. conduct a thorough risk-based analysis of the functions that are being considered for an arrangement with a TPSP or have been provided by a TPSP, whether the functions are critical or important and address the potential risks, in particular the operational and reputational risks, and the oversight limitations related to the countries where the functions are or may be provided;

b. consider the consequences of where the TPSP is located (within or outside the EU);

c. consider the political stability and security situation of the jurisdictions in question, including:

i. the laws in force, including laws on data protection, compliant with the EU General Data Protection Regulation (GDPR);

ii. the law enforcement provisions in place; and

iii. the insolvency law provisions that would apply in the event of a TPSP's failure and any constraints that would arise in respect of the urgent recovery of the financial entity's function in particular;

d. consider whether the TPSP is a subsidiary or parent undertaking of the financial entity, is included in the scope of accounting consolidation or is a member of or owned by financial entities that are members of an institutional protection scheme and, if so, the extent to which the financial entity controls it or has the ability to influence its actions in line with Section 2.

11.3 Due diligence

79. Before entering into third-party arrangements and considering all the relevant risks related to the function that will be performed by a TPSP, financial entities should ensure in their selection and assessment process that the prospective TPSP is suitable and that the level of details regarding the due diligence is proportionate to the criticality or importance of the relevant function.

80. Factors to be considered when conducting due diligence on a potential TPSP include, but are not limited to:

    a. its business model, nature, scale, complexity, financial soundness, ownership and group as well as organisational structure;

    b. operational and technical capability and track record, including, where possible, drawing on prior engagements or potential long relationships between the financial entity and the TPSP;

    c. whether the TPSP is a parent undertaking or subsidiary of the financial entity, is part of the accounting scope of consolidation of the institution or is a member of or is owned by institutions that are members of the same institutional protection scheme to which the institution belongs;

    d. whether or not the TPSP is supervised by competent authorities.

81. With regard to critical and important functions[63], financial entities should ensure that the TPSP has:

    a. the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources (e.g. human, ICT, financial) to deliver the relevant service;

    b. appropriate internal controls and risk management processes and procedures, including its ability to manage operational risks, especially supply chain risks when applicable;

    c. geographic dependencies and management of related risks. These risks may relate to the economic, financial, political, legal and regulatory environment in the jurisdiction(s) where the relevant service will be provided;

    d. business continuity plans, contingency plans, disaster recovery plans and other relevant plans;

[63] Without prejudice of the conditions listed in Article 31(2) of Commission Delegated Regulation (EU) 2017/565.

e. if applicable, the required regulatory authorisation(s) or registration(s) to perform the critical or important function in a reliable and professional manner to meet its obligations over the duration of the contract;

f. proper arrangements that ensure that it is effectively possible to conduct audits, including onsite, by the financial entity itself, appointed third-parties, and competent authorities at the TPSP.

The planned usage of subcontractors to perform services supporting critical or important functions or material parts thereof, is also to be considered.

82. Where the use of a TPSP involves the processing of personal or confidential data, financial entities should be satisfied that the TPSP implements appropriate technical and organisational measures to protect the data.

83. Financial entities should take appropriate steps to ensure that the TPSPs act in a manner consistent with their values and code of conduct. In particular, with regard to TPSPs located in third countries and, if applicable, their subcontractors, financial entities should be satisfied that such TPSP acts in an ethical and socially responsible manner, including by taking into account environmental, social and governance (ESG) risks, and adheres to international standards on human rights (e.g. the European Convention on Human Rights), environmental protection and appropriate working conditions, including the prohibition of child labour.

12 Contractual phase

84. The rights and obligations of the financial entity and the TPSP should be clearly allocated and set out in one written agreement, available to the parties on paper or electronically in a durable, immutable and accessible format.

85. The third-party agreement should include at least the following elements:

a. a clear and complete description of all functions to be provided by the TPSP, indicating whether the subcontracting of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in Section 12.1 that the subcontracting is subject to;

b. the location(s) (i.e. regions or countries) where the function will be provided, and the conditions to be met, including a requirement to notify the financial entity if the TPSP envisages to change the location(s);

c. the location where the data is processed including storage;

d. the start date and end date, where applicable, of the agreement;

e. the governing law of the agreement;

f. the parties' financial obligations;

g. provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;

h. provisions that ensure that the data that are owned by the financial entity can be accessed, recovered and returned in the case of the insolvency, resolution or discontinuation of business operations of the TPSP, or in the event of the termination of the contractual arrangements;

i. service level descriptions, including their updates and revisions thereof;

j. the right of the financial entity to monitor the TPSP's performance on an ongoing basis;

k. the obligation of the TPSP to fully cooperate with the competent authorities and resolution authorities of the financial entity, including other persons appointed by them;

l. termination rights and related notice periods for the termination of the third-party arrangement, as specified in Section 12.4;

m. for institutions under CRD, a clear reference to the national resolution authority's powers, especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the 'substantive obligations' of the contract in the sense of Article 68 of that Directive.

86. In addition to the elements referred to in paragraph 85, the third-party arrangement for critical or important functions should set out at least:

a. the agreed service level descriptions, including their updates and revisions thereof, with precise quantitative and qualitative performance targets for the function provided to allow for effective timely monitoring by the financial entity so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;

b. the notice periods and reporting obligations of the TPSP to the financial entity, including the communication by the TPSP of any development that may have a material impact on the TPSP's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the TPSP

c. whether the TPSP should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

d. the requirements for the TPSP to implement and test business contingency plans;

e. the right of the financial entity to monitor the TPSP's performance on an ongoing basis, which entails the following:

   i. the unrestricted right of financial entities and competent authorities to inspect and audit the TPSP, as specified in Section 12.1;

   ii. the right to agree on alternative assurance levels if other clients' rights are affected;

   iii. the obligation of the TPSP to fully cooperate during the onsite inspections and audits performed by the competent authorities, the financial entity or an appointed third-party; and

   iv. the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;

f. exit strategies, in establishment of a mandatory adequate transition period:

   i. during which the TPSP will continue providing the respective functions with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring; and

   ii. allowing the financial entity to migrate to another TPSP or change to in-house solutions consistent with the complexity of the service provided.

87. Without prejudice to the requirements under the Regulation (EU) 2016/679, financial entities, when contracting with TPSPs, located, in particular in third countries, should take into account differences in national provisions regarding the protection of data. Financial entities should ensure that the third-party arrangement includes the obligation that the TPSP protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the financial entity (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).

12.1 Subcontracting of critical or important functions

88. The third-party arrangement should specify whether subcontracting of critical or important functions, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting. The use of subcontractors providing or supporting critical or important functions by TPSPs cannot reduce the ultimate responsibility for the management body of the financial entities to manage their risks and to comply with their legislative and regulatory obligations. Financial entities should have a clear and holistic view of the risks associated with subcontracting services that support critical or important functions so that they are able to monitor, manage and mitigate those risks.

89. If subcontracting of critical or important functions or material part thereof is permitted, financial entities should determine whether the function to be subcontracted is, as such, critical or important and, if so, record it in the register.

90. If subcontracting of critical or important functions or material part thereof is permitted, the written agreement between the financial entity and the TPSPs should specify:

    a. any types of activities that are excluded from subcontracting;

    b. the conditions to be complied with in the case of subcontracting;

    c. that the TPSP has to assess all risks associated with the location of the current or potential subcontractors that provide or support critical or important functions, and their parent company and with the location where the function concerned is provided from;

    d. that the TPSP is obliged to monitor those function that it has sub-contracted to ensure that all contractual obligations between the TPSP and the financial entity are continuously met;

    e. the reporting obligations of the TPSP towards the financial entity regarding subcontractors that provide or support critical or important functions;

    f. that the TPSP has to specify in its contract with its subcontractors the monitoring and reporting obligations of that subcontractor towards the TPSP, and where agreed, towards the financial entity;

    g. that the TPSP has to ensure the continuity of the critical or important functions throughout the chain of subcontractors in case of failure by a subcontractor to meet its contractual obligations;

    h. that the subcontractor has to grant to the financial entity and relevant competent and resolution authorities the same rights of access, inspection, and audit as those granted by the TPSP to the financial entity; and

    i. that the TPSP has to notify the financial entity of any material change to subcontracting arrangements.

    Changes relative to written agreements between the financial entity and the TPSP that support critical or important functions and made necessary to comply with these Guidelines, should be implemented in a timely manner and as soon as it is possible. The financial entity should document the planned timeline for the implementation.

91. The written agreement between the financial entities and the TPSPs should specify that the TPSP should inform the financial entity about any intended material changes to its subcontracting arrangements well in time to enable the financial entity to assess:

    - the impact on the risks it is or might be exposed to;

- whether such material changes might affect the ability of the TPSP to meet its contractual obligations *vis-a-vis* the financial entity.

92. The written agreement should include a reasonable notice period by which the financial entity is able to approve or to object to the changes.

93. The TPSP should only implement the material changes to its subcontracting arrangements after the financial entity has either approved or not objected to the changes by the end of the notice period.

94. Where the financial entity is of the opinion that the material changes referred to in paragraph 91 exceed the financial entity's risk tolerance, the financial entity should before the end of the notice period:

    - inform the TPSP thereof; and

    - object to the changes and request modifications to those changes before they are implemented.

95. Financial entities should ensure that the TPSP appropriately identifies all subcontractors and monitors subcontractors providing critical or important functions or material parts thereof, in line with its contractual obligations defined by the financial entity.

96. The financial entity should have the right to provide in the written agreement with the TPSP that the agreement is to terminate in each of the following cases:

    - the financial entity has objected to material changes to the subcontracting arrangements supporting critical or important functions and requested for modifications to those arrangements, but the TPSP has nevertheless implemented those material changes;

    - the TPSP has implemented material changes to subcontracting arrangements supporting critical or important functions before the end of the notice period without approval by the financial entity;

    - the TPSP subcontracts a function that supports a critical or important function not explicitly permitted to be subcontracted by the contract between the financial entity and the TPSP.

12.2 Access, information and audit rights

97. Financial entities should ensure through the written third-party arrangement that the internal audit function is able to review the function performed by the TPSP using a risk-based approach.

98. Regardless of the criticality or importance of the function performed by TPSPs, the written third-party arrangements between institutions under CRD and TPSPs should refer to the information gathering and investigatory powers of competent authorities and resolution authorities under Article 63(1)(a) of Directive 2014/59/EU and Article 65(3) of Directive 2013/36/EU with regard to TPSPs located in a Member State and should also ensure those rights with regard to TPSPs located in third countries.

99. With regard to the provision of critical or important functions by the TPSP, financial entities should ensure within the written third-party arrangement that the TPSP grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following:

    a. full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the function, including related financial information, personnel and the TPSP's external auditors ('access and information rights'), as well as taking copies of relevant information and documentation; and

    b. unrestricted rights of inspection and auditing related to the third-party arrangement ('audit rights'), to enable them to monitor the third-party arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

100. For the provision of functions that are not critical or important by TPSPs, financial entities should consider including the access and audit rights as set out in paragraph 99 (a) and (b) and Section 12.2, on a risk-based approach, taking into account the nature of the function and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. Financial entities should take into account that functions may become critical or important over time.

101. Financial entities should ensure that the third-party arrangement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights, where granted, by them, competent authorities or third-parties appointed by the financial entity or competent authorities to exercise such rights.

102. Financial entities should exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards[64].

103. Without prejudice to their final responsibility regarding third-party arrangements, financial entities may use:

[64] For institutions, please refer to Section 22 of the EBA Guidelines on internal governance: https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf/eb859955-614a-4afb-bdcd-aaa664994889

a. pooled audits organised jointly with other clients of the same TPSP and performed by them and these clients or by a third-party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the TPSP;

b. third-party certifications and third-party or internal audit reports, made available by the TPSP.

104. For the provision of critical or important functions by TPSPs financial entities should assess whether third-party certifications and third-party or internal audit reports as referred to in paragraph 103(b) are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these certifications and reports over time. When relying on pooled audits as referred to in paragraph 103(a), financial entities should assess whether they have sufficient information and are sufficiently involved in scoping, planning, performing and reporting the audit.

105. Financial entities should make use of the method referred to in paragraph 103(b) only if they:

a. are satisfied with the audit plan for the function provided by TPSPs;

b. ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the financial entity and the compliance with relevant regulatory requirements;

c. thoroughly assess the content of the certifications or audit reports, on an ongoing basis and verify that the reports or certifications are not obsolete;

d. ensure that key systems and controls are covered in future versions of the certification or audit report;

e. are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);

f. are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;

g. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective; and

h. retain the contractual right to perform individual audits at their discretion with regard to the use of TPSPs for the provision of critical or important functions.

106. Before a planned on-site visit, financial entities, competent authorities and auditors or third-parties acting on behalf of the financial entity or competent authorities should provide reasonable notice to the TPSP, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.

107. When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.

108. Where the third-party arrangement carries a high level of technical complexity, the financial entity should verify that whoever is performing the audit – whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the financial entity reviewing third-party certifications or audits carried out by TPSP.

12.3 Termination rights

109. The financial entities should be able to terminate the third-party arrangement where necessary, in accordance with applicable law, including in the following situations:

a. where the TPSP of the functions is in a breach of applicable law, regulations or contractual provisions;

b. where impediments capable of altering the performance of the function provided by a TPSP are identified;

c. where there are material changes affecting the third-party arrangement or the TPSP (e.g. subcontracting or changes of subcontractors);

d. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information;

e. where instructions are given by the financial entity's competent authority, e.g. in the case that the competent authority is, caused by the third-party arrangement, no longer in a position to effectively supervise the financial entity.

110. The third-party arrangement should facilitate the transfer of the function provided by the TPSP to another TPSP or its re-incorporation into the financial entity. To this end, the written third-party arrangement should:

a. clearly set out the obligations of the existing TPSP in the case of a transfer of the function provided by the TPSP to another TPSP or back to the financial entity, including the treatment of data;

b. set an appropriate transition period, during which the TPSP, after the termination of the arrangement, would continue to provide the function performed to reduce the risk of disruptions; and

c. include an obligation of the TPSP to support the financial entity in the orderly transfer of the function in the event of the termination of the third-party arrangement.

13 Monitoring

111. Financial entities should monitor, on an ongoing basis, the performance of the TPSPs with regard to all third-party arrangements on a risk-based approach and with the main focus being on the third-party arrangements of critical or important functions, including that the availability, integrity and security of data and information is ensured. Where the risk, nature or scale of a function performed by a TPSP has materially changed, financial entities should reassess the criticality or importance of that function in line with Section 4.

112. Financial entities should apply due skill, care and diligence when monitoring and managing third-party arrangements.

113. Financial entities should regularly update their risk assessment in accordance with Section 11.2 and should periodically report to the management body on the risks identified in respect of the third-party arrangements of critical or important functions.

114. Financial entities should monitor and manage their internal concentration risks caused by third-party arrangements, taking into account Section 11.2 of these Guidelines.

115. Financial entities should ensure, on an ongoing basis, that third-party arrangements, with the main focus being on third-party arrangements for critical or important functions, meet appropriate performance and quality standards in line with their policies by:

a. ensuring that they receive appropriate reports from TPSPs;

b. evaluating the performance of TPSPs using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and

c. reviewing all other relevant information received from the TPSP, including reports on business continuity measures and testing.

116. Financial entities should take appropriate measures if they identify shortcomings in the provision of the function performed by a TPSP. In particular, financial entities should follow up on any indications that TPSPs may not be carrying out the critical or important function effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, financial entities should take appropriate corrective or remedial actions. Such

actions may include terminating the third-party arrangement, with immediate effect, if necessary.

14 Exit strategies

117. Financial entities should have a documented exit strategy when critical or important functions are performed by TPSPs that is in line with their policy on third-party risk management and business continuity plans[65], taking into account at least the possibility of:

a. the termination of third-party arrangements;

b. the failure of the TPSP;

c. concentration risk at entity level and the possibility of difficult exit;

d. the deterioration of the quality of the function provided and actual or potential business disruptions caused by the inappropriate or failed provision of the function;

e. material risks arising for the appropriate and continuous application of the function;

f. significant breach by the TPSP of applicable laws, regulations or contractual terms.

118. Financial entities should ensure that they are able to exit third-party arrangements without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of its provision of services to clients. To achieve this, they should:

a. develop and implement exit plans that are realistic, feasible, based on plausible scenarios and reasonable assumptions. Exit plans should be comprehensive, documented and, where appropriate, sufficiently tested (e.g. by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring a service performed by a TPSP to an alternative provider; and

b. identify alternative solutions and develop transition plans to enable the financial entity to remove functions provided by TPSPs and data from the TPSP and transfer them to alternative TPSPs or back to the financial entity or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.

119. When developing exit strategies, financial entities should:

a. take into account the results of the analysis described in paragraph 75;

[65] Institutions, in line with Title VI of the EBA Guidelines on internal governance, should have appropriate business continuity plans in place with regard to the provision of critical or important functions by third-party service providers.

b. define the objectives of the exit strategy;

c. perform a business impact analysis that is commensurate with the risk of the processes, services or activities provided by TPSPs, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take. This should be subject to a regular review taking into account the current situation;

d. assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;

e. define success criteria for the transition of functions provided by TPSPs and data; and

f. define the indicators to be used for the monitoring of the third-party arrangement (as outlined under Section 13), including indicators based on unacceptable service levels that should trigger the exit.

Question n. 4

Is Title IV of the Guidelines appropriate and sufficiently clear?

Title V – Guidelines on third-party risks arrangements addressed to competent authorities

120. When establishing appropriate methods to monitor financial entities' compliance with the conditions for initial authorisation, competent authorities should aim to identify if third-party arrangements amount to a material change to the conditions and obligations of institutions' and payment institutions' initial authorisation.

121. Competent authorities should be satisfied that they can effectively supervise financial entities, including that financial entities have ensured within their third-party arrangement that TPSPs are obliged to grant audit and access rights to the competent authority and the entity, in line with Section 12.2.

122. The analysis of financial entities' third-party risk should be performed at least within the SREP or, with regard to payment institutions, as part of other supervisory processes, including ad-hoc requests, or during on-site inspections.

123. Further to the information recorded within the register, as referred to in Section 10, competent authorities may ask financial entities for additional information, in particular for arrangements with TPSPs for the provision of critical or important function, such as:

a. the detailed risk analysis;

b. whether the TPSP has a business continuity plan that is suitable for the services provided to the financial entity;

c. the exit strategy for use if the third-party arrangement is terminated by either party or if there is disruption to the provision of the services; and

d. the resources and measures in place to adequately monitor the activities performed by TPSPs.

124. In addition to the information required under Section 10, competent authorities may require financial entities to provide detailed information on any third-party arrangement, even if the function concerned is not considered critical or important.

125. Competent authorities should assess the following on a risk-based approach:

a. whether financial entities monitor and manage appropriately, in particular arrangements with TPSPs for the provision of critical or important functions;

b. whether financial entities have sufficient resources in place to monitor and manage third-party arrangements;

c. whether financial entities identify and manage all relevant risks; and

d. whether financial entities identify, assess and appropriately manage conflicts of interest with regard to any third-party arrangement, e.g. in the case of intragroup agreements or arrangements within the same institutional protection scheme.

126. Competent authorities should ensure that EU/EEA financial entities are not operating as an 'empty shell', including situations where financial entities use back-to-back transactions or intragroup transactions to transfer part of the market risk and credit risk to a non-EU/EEA entity, and should ensure that they have appropriate governance and risk management arrangements in place to identify and manage their risks.

127. Within their assessment, competent authorities should take into account all risks, in particular:[66]

a. the operational risks posed by the third-party arrangement;

b. reputational risks;

c. the step-in risk that could require the institution to bail out a TPSP, in the case of significant institutions;

d. concentration risks within the institution, including on a consolidated basis, caused by multiple third-party arrangements with a single TPSP or closely connected TPSPs or multiple third-party arrangements within the same business area;

[66] For institutions subject to Directive 2013/36/EU, see also the EBA Guidelines on SREP: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2.

e. concentration risks at the sector level, e.g. where multiple financial entities make use of a single TPSP or a small group of TPSPs;

f. the extent to which the financial entity controls the TPSP or has the ability to influence its actions, the reduction of risks that may result from a higher level of control and if the service provider is included in the consolidated supervision of the group; and

g. conflicts of interest between the financial entity and the TPSP.

128. Where concentration risks are identified, competent authorities should monitor the development of such risks and evaluate both their potential impact on other financial entities and the stability of the financial system. Moreover, competent authorities should inform, where appropriate, the resolution authority about new potentially critical functions[67] that have been identified during this assessment.

129. Where concerns are identified that lead to the conclusion that a financial entity no longer has robust governance arrangements in place or does not comply with regulatory requirements, competent authorities should take appropriate actions, which may include limiting or restricting the scope of the functions performed by TPSPs or requiring exit from one or more third-party arrangements. In particular, taking into account the need of the financial entity to operate on a continuous basis, the termination or the temporary suspension of contracts could be required if the supervision and enforcement of regulatory requirements cannot be ensured by other measures.

130. Competent authorities should be satisfied that they are able to perform effective supervision, in particular when critical or important functions for financial entities are performed by TPSPs and undertaken outside the EU/EEA.

131. Competent authorities should closely cooperate among themselves and should, in a timely manner, mutually exchange all relevant information, especially concerning critical or important functions provided by TPSPs which is necessary for them to carry out their respective duties under this Title V, including in relation to concentration risk at sector level.

[67] As defined under Article 2(1)(35) BRRD.

Annex I
Non exhaustive list of functions that could be provided by a third-party service provider

This list is to be used for classification by financial entities and should only be considered as a list of non-exhaustive examples. Financial entities are encouraged to maintain their own classification rather than using those examples set out in the Annex, if more relevant or appropriate.

Level 1 Category	Level 2 Category
Administrative services	• Advertising & Marketing; • Document Management & Archiving; • Insurance Services; • Payroll Services; • Pensions & benefits; • Postal services & Mailing; • Procurement & purchasing of services; • Secretarial Services; • Talent acquisition & hiring; Travel & Entertainment Services; Other
Cash Management Services	• Automatic Teller Machine servicing & maintenance; • Cash processing & transport; • Cash vault services; • Foreign banknote management; • Other
Customer services	• Customer complaint management; • Customer contact services & call centre; • Customer relationship management services; • Marketing; • Product design, management, and advice; • Sales; • Other
Depositary tasks & administration for UCI	• Administration for UCI - Client communication function; • Administration for UCI - NAV calculation and accounting function; • Administration for UCI - Registration function; • Depositary tasks for UCI - Cash flow monitoring; • Depositary tasks for UCI - Oversight duties; • Depositary tasks for UCI - Safekeeping duties; • Other
Finance, Treasury, Accounting and Reporting	• Accounting – Advisory & accounting expertise; • Accounting – Annual, quarterly and monthly reports; • Accounting – Other; • Accounting – Recording of accounting transactions, reconciliation, and bookkeeping; • Financial & Capital Management Services; Reporting – Financial Investigations & transaction reporting (non-AML); • Reporting – Management & Strategic Planning, Business Intelligence & Analysis; • Reporting – Regulatory & Supervisory; • Reporting – Statutory Reporting & Disclosure; • Treasury & Liquidity Management Services; • Other

Internal control functions	• Business Continuity Management; • Compliance function (non-AML); • Data Protection Officer & Management; • Disaster Recovery Management; • Financial & Earnings Controlling; • First Line of Defence Controls; • Internal audit function; • Market Abuse Control Functions; • Risk management function – Counterparty risk management; • Risk management function – Credit risk management; • Risk management function – Incident management (non-IT); • Risk management function – Interest rate risk management; • Risk management function – Internal model development and maintenance
Investment services	• Advice to undertakings and advice relating to mergers and purchase of undertakings; • Ancillary services related to underwriting; • Functions related to dealing on own account; • Functions related to the execution of orders on behalf of clients; • Foreign exchange services connected to the provision of investment services; • Granting credits or loans to an investor to allow him to carry out a transaction in one or more financial instruments; • Functions related to the provision of investment advice; • Investment research and financial analysis or other forms of general recommendation; • Investment services and activities as well as ancillary services related to the underlying of the derivatives where these are connected to the provision of investment or ancillary services; • Functions related to the operation of a Multilateral Trading Facility; • Functions related to the operation of an Organised Trading Facility; • Functions related to placing of financial instruments without a firm commitment basis; • Functions related to the portfolio management
Lending	• Client acquisition, sales & origination; • Collateral valuation, collateral management and sale; • Credit & repayment monitoring; • Credit administration & other back-office functions; • Credit decision-making; • Credit renewal and refinancing; • Credit scoring & solvency analysis; • Customer administration for after-sales events; • Debt collection and recovery services; • Preparation of contracts and document management; • Other
Payment services	• Authentication & authorisation; • Execution of credit transfers (including standing orders); • Execution of payment transactions – execution of direct debits; • Execution of payment transactions – through cheques; • Execution of payment transactions – through payment cards or similar device; • Handling of failed processing and incorrect transactions (including chargebacks and restitution); • Interbank payments; • Issuing of payment instruments and/or acquiring of payment transactions; • Money remittance; • Payment channels; • Processing of trade finance transactions; • Other

Securities	• Asset servicing; • Brokerage; • Clearing, settlement & reconciliation; • FX business; • Proxy voting; • Safekeeping and Custodianship; • Trustee, depositary & fiduciary services; • Valuation services; • Other
ART issuance	• Operating the reserve of assets; • Investment of the reserve of assets; • Custody of the reserve of assets; • Distribution of the ART to the public (where applicable); • Other
Other	Other

Question n. 5

Is Annex I, provided as a list of non-exhaustive examples, appropriate and sufficiently clear?

5. Accompanying documents

5.1 Draft cost-benefit analysis/impact assessment

Article 16(2) of 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) (the EBA Regulation) provides that the EBA should carry out an analysis of 'the potential related costs and benefits' of any guidelines it develops. This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options.

A. Problem identification

The EBA guidelines on outsourcing, published in March 2019, specify the internal governance arrangements, including sound risk management, that should be implemented in connection with the outsourcing of functions (i.e. activity, service or process) (or a part thereof) and the criteria to assess whether an outsourced function is critical or important. Since their publication, those Guidelines apply not only to credit institutions and investment firms that were subject to Directive 2013/36/EU (CRD), but also to payment institutions (PIs) and electronic money institutions (EMIs) (within the scope of Directive (EU) 2015/2366 and Directive 2009/110/EC) when they outsource functions. They also integrate the EBA recommendation on outsourcing to cloud service providers, published in December 2017.

Following the entry into force of Directive 2024/1619/EU (CRD), Directive 2019/2034/EU (IFD), Regulation (EU) 2023/1114 (MICAR), Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), those Guidelines on outsourcing need to be updated to develop a more general approach on the management of third-party risks.

In addition, the work at international level should also be considered, in particular the FSB toolkit on third-party risk management published in December 2023[68] and the BCBS work on third-party risk management[69].]

B. Policy objectives

To ensure a level playing field and to meet the requirements under CRD, IFD, MiFID II, PSD2, EMD, and MiCAR, and to take into account the entry into force of DORA, the EBA is now updating the

[68] See: Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities (fsb.org).

[69] See: BCBS core principles in particular Principle 25 (www.bis.org/bcbs/publ/d551.pdf) and the Principles for the sound management of third-party risk (currently under development).

Guidelines on outsourcing issued in 2019 to establish one common framework for the management of third-party risk of non-related ICT services by all financial institutions within the scope of the EBA's action. Hence, the use of ICT third-party service providers providing ICT services, including when supporting critical or important functions, should be excluded from the Guidelines' scope of application as it is already covered under DORA. However, the link between the existing outsourcing framework as a subset of third-party risk management framework is clarified and continue to exist.

To cater for the principle of proportionality, the Guidelines require to identify the provision of critical or important functions by third-party service providers (TPSPs) to financial entities and impose stricter requirements compared with other third-party arrangements.

The Guidelines aim to clarify the supervisory expectations regarding TPSPs, including service providers located in third countries, to ensure that third-party arrangements are concluded and performed in an orderly manner and do not lead to the setting up of empty shells that no longer have the substance to remain authorised.

The Guidelines aim to ensure that competent authorities are able to identify concentrations of third-party arrangements at TPSPs based on documentation provided by financial entities, to identify and manage risks to the stability of the financial system.

C. Baseline scenario

Directive 2013/36/EU (CRD) strengthens the governance requirements for institutions and Article 74(3) CRD gives the EBA the mandate to develop guidelines on institutions' governance arrangements. As part of institutions' governance arrangements, which include effective processes to identify, manage, monitor and report the risks they are or they might be exposed to, including third-party risk. Besides, Article 76 CRD sets out requirements for the involvement of the management body in risk management and Article 88 CRD sets out the responsibilities of the management body regarding governance arrangements; in both cases, the requirements are relevant for third-party risk management.

Directive 2019/2034/EU (IFD) sets out requirements for internal governance of investment firms which are not small and interconnected under Article 12(1) of Regulation (EU) 2019/2033 and give EBA, in consultation with ESMA, the mandate to issue guidelines in this area[70] while Regulation (EU) 2023/1114 (MiCAR) sets out a specific mandate for the EBA in consultation with ESMA and ECB to develop guidelines on internal governance regarding issuers of ARTs. Directive 2014/65/EU (MiFID II) contains also explicit provisions regarding the outsourcing of operational functions in the field of investment services and activities. Directive 2015/2366/EU (PSD2) sets out requirements for the outsourcing of functions by payment institutions.

Financial entities must ensure that sensitive data, including personal data, is adequately protected and kept confidential. Financial entities must comply with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (repealing Directive 95/46/EC).

[70] See Final Report on GL on internal governance under IFD.pdf (europa.eu)

All of the above forms the baseline scenario of the impact assessment, which focuses only on the additional costs and benefits created by the Guidelines on third-party risk management.

D. Options considered

1) Scope of application

Option A: applying the Guidelines only to initial addressees (ie credit institutions and investment firms subject to the CRD, payment institutions (PIs) under PSD2 and electronic money institutions (EMIs) under EMD as in the previous Guidelines on outsourcing).

Option B: extending the scope of the Guidelines to investment firms under IFD, non-credit institutions under MCD and issuers of ARTs (if not within CRD scope), taking into account of the application of the proportionality principle.

Institutions under CRD (ie credit institutions and investment firms) will continue to be subject to the GLs as they are required under Article 74 of CRD to have sound governance arrangements and to manage all their risks including the third-party risk. PIs and EMIs should continue to be under the scope of the GLs as in accordance with Article 5(1) of PSD2, PIs/EMIs should have sound governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures". This provision allows PIs/EMIs to be maintained in the scope of these guidelines as the management of third-party risk is also part of sound governance arrangements. However, limiting the scope only to these institutions (Option A) would potentially lead to inconsistencies between the different frameworks and to a situation unlevel playing field between investment firms within CRD's scope and the others within IFD's scope, ART issuers within CRD's scope and the others, and non-credit institutions. In particular, those institutions would need to implement separate arrangements for the different types of activities.

Besides, while all investment firms are subject to MiFID which sets out requirements on outsourcing, a prudential framework for investment firms has been introduced in 2019 with Directive 2019/2034/EU (IFD). In accordance with this framework Class 2 are covered by IFD provisions requiring them to have sound governance arrangements (Article 26 of IFD) and should therefore be covered by the GLs. Thus, only small and non-interconnected investment firms under Article 12(1) of Regulation (EU) 2019/2033 (Class 3) should be excluded from the scope of those GLs.

Directive 2014/17/EU (MCD) defines non-credit institutions as "*any creditor that is not a credit institution*" (Art. 4, point 10 of MCD). Additionally, "creditor" means a natural or legal person who grants or promises to grant credit falling within the scope of Article 3 in the course of his trade, business or profession (Art. 4, point 2 of MCD). Even if there are no provisions regarding governance or outsourcing arrangements under the MCD, they should also be included within the GLs' scope to ensure a level playing field, also considering that a specific section on outsourcing is already included in the EBA GL on arrears and foreclosure (referring to the former CEBS guidelines on outsourcing).

Following the entry into force of Regulation (EU) 2023/1114 (MiCAR), issuers of ARTs that are not credit institutions (legal person or other undertaking) should also be included within the scope of

the Guidelines to ensure a level playing field with credit institutions that issue ARTs which are already in the scope the Guidelines. Moreover, issuers of ART are subject to sound governance arrangements under Article 34 of MiCAR including the sound management of third-party risks.

Option B has been retained.

2) Transitional arrangements

Option A: setting an implementation period of the Guidelines of one year, but without transitional arrangements.

Option B: setting out transitional arrangements to ensure that financial entities can review contracts, update the assessment of the criticality or importance related to their third-party arrangements (TPA), set up the register of non-ICT related services TPA and update the documentation in line with the guidelines.

Option B1: setting a fixed transitional period of two years to review contracts, perform assessments and complete the register for non-ICT TPA.

Option B2: setting a period of two years but requiring assessments to be updated if existing TPA are renewed during that period and to update the register for non-ICT TPA. For critical or important functions under third-party arrangements, closer supervisory attention should be applied and, after the transitional period, their reassessment should be monitored.

All options would be effective to achieve the desired prudential outcome to have all third-party arrangements documented in a way that differentiates between critical and important functions, setting out a framework for such third-party arrangement and allowing for the submission of a register to competent authorities.

Option A would lead to time pressure to re-assess the criticality or importance of third-party arrangements and update the register for non-ICT TPA and this option might therefore increase the implementation costs. In addition, it might not be possible to renegotiate multiple third-party arrangements in a relatively short time period. Therefore, Option A has not been retained.

Both options B1 and B2 would ensure that financial entities have sufficient time to update their assessments and documentation. However, Option B1 would raise challenges, as contracts would need to be renegotiated within that time period, which may not always be possible.

Option B2 would lead to a faster update than Option B1 for arrangements that are renewed during the transitional period, but without additional burden, as an assessment of renewed third-party arrangements would include the assessment of the related risks. Updating the documentation in that context would be possible without causing material additional costs. Option B2 would have some impact on the available time frame for the development of a database that could hold the register for non-ICT TPA. However, for this task, the regular implementation period should be sufficient, as such register might already exist at least for outsourcing arrangements. Additional scrutiny would be applied to critical or important functions provided by TPSPs that are updated only after the transitional period. While this would lead to additional costs for competent authorities for the monitoring of the transition, it would reduce the costs for financial entities, as the time pressure for renegotiation of contracts or, in some cases, exit from third-party

arrangements (where there is no renegotiation possible that ensures compliance with the Guidelines) would be reduced.

Option B2 has been retained, as it provides more flexibility but still ensures the effective supervision of third-party arrangements.

3) Definition of third-party arrangements and the identification of critical and important functions provided by third-party service providers

Option A: relying on the definition provided in Basel framework and the FSB toolkit, specifying that outsourcing arrangement are a subset of those TPA, and the approach to set stricter requirements for critical and important functions.

Option B: the same as Option A but also setting a lighter framework for other third-party arrangements.

Using a common definition (Option A) ensures that financial entities can implement a single framework for third-party arrangements regarding all of their activities. A focus on the critical or important functions provided by TPSPs should reduce the administrative costs of applying the Guidelines. However, the assessment of the criticality or importance includes judgemental elements and therefore financial entities, and competent authorities may sometimes disagree regarding the assessment result. Retroactively introducing safeguards for the critical or important functions provided by TPSPs, also in cases where the assessment changes over time, could lead to additional costs and situations where necessary contractual changes are difficult to agree on. In addition, the overall impact of third-party arrangements that are themselves not critical or important might become relevant for the supervision of a financial entity.

Under Option B, the impact described under Option A would apply; in addition, some guidelines for all third-party arrangements would be imposed, taking into account the principle of proportionality. This would lead to only a minor additional administrative burden, as financial entities would already need to have in place some processes to manage all of their arrangements with TPSPs. In any case, also for other third-party arrangements, financial entities would already need to apply sound processes and would need to document the arrangements to ensure that they have robust governance arrangements in place. Having guidelines in place that specify the regulatory minimum expectations for such non-critical or non-important arrangements would provide a higher level of legal certainty. Costs for adjustments of internal processes should be minor.

Option B has been retained.

4) Specification of the basic requirements on governance arrangements, third-party risk policy, conflicts of interest, business continuity and internal audit function that are, in principle, covered already in the EBA Guidelines on internal governance and were already covered in the EBA outsourcing guidelines

Option A: the Guidelines should not further specify such requirements, as the EBA Guidelines on internal governance are sufficient and the EBA guidelines already covered those for outsourcing arrangements.

Option B: the Guidelines should specify further the additional aspects that are specific to third-party arrangements.

0ption A would not provide legal certainty in the same way as Option B.

The further specifications (Option B) provide for certainty regarding the supervisory expectations and ensures that there are sufficient governance arrangement within financial entities not covered by the CRD, since the scope of the Guidelines has been broadened (see Policy issue n°1); this option also provides legal certainty and clarity regarding supervisory expectations for institutions subject to the CRD. This is desirable to achieve further harmonisation and supervisory convergence. In relation to business continuity plans (Section 8), the Section has been streamlined and a cross reference to the EBA Guidelines on internal governance under Directive 2013/36/EU has been made.

Option B has been retained.

5) Documentation requirements and the submission of documentation to competent authorities

Documentation should be comprehensive, provide an appropriate overview on third-party arrangements for non-ICT services (including the main risks identified regarding the critical and important functions provided by TPSPs) and allow for the identification of concentration risks at micro level by financial entities and at macro level by competent authorities. The guidelines on outsourcing already required the implementation of a register of all outsourcing arrangements. DORA also requires the setting up of a register (see DORA ITS on register of information). While the documentation regarding third-party arrangements needs to be extended beyond outsourcing arrangements, ICT third-party arrangements have to be documented under the DORA framework. Several options have been considered.

Option A: requiring financial entities to document all third-party arrangements, but without specifying further requirements.

Option B: requiring financial entities to document in a specific register all third-party arrangements for non-ICT services, taking into account DORA's register for ICT services.

Option B1: limiting the register to only the critical and important functions provided by TPSPs for non-ICT services.

Option B2: having all third-party arrangements for non-ICT services documented in the register, but with more specific requirements for critical or important functions.

Option C: the same as Option B but requiring that planned third-party arrangements for non-ICT services also have to be documented in the register as soon as their implementation is likely.

Option D: the same as Option B, but with the possibility that the non-ICT register under those GL and the ICT register under DORA might be merged, where relevant and under the FE's discretion

Option A would not necessarily result in a comprehensive register that would be readily available for submission to the competent authority and would allow neither financial entities nor their competent authorities to efficiently identify risk concentrations and operational resilience. Besides, such option would be redundant with the DORA register. Option A therefore has not been retained.

Option B would ensure that financial entities and competent authorities have an overview of all relevant third-party arrangements with non-ICT services and would be in a position to assess risk concentrations and ensure their operational resilience. By defining a minimum set of aspects to be documented, this option would ensure that there is sufficient information available to assess the risk posed by third-party arrangements, e.g. within the SREP. The information should be limited to reduce the burden. Additional information could always be requested by competent authorities. taking into account the application of DORA; consistency between the two registers need to be ensured and financial entities should be encouraged to have consistent information in those registers (both for ICT and non-ICT services). Option B also facilitates the use of this information by competent authorities.

Option B1 would lead to slightly lower costs, as not all of third-party arrangements would need to be included in the register. However, documentation would be necessary in any case, and such option won't be consistent with the DORA register which captured all ICT third-party agreements. By including at least, a limited set of information (Option B2) for all third-party arrangements, the implementation of the register for non-ICT services and the identification of concentration risks would be even better than in Option B1. Having specific requirements for critical or important functions would also make Option B2 more efficient than Option B1, and much more consistent with DORA register.

Adding planned third-party arrangements to the register (Option C) would give competent authorities the possibility to evaluate the potential effect of upcoming third-party arrangements for non-ICT services combined with other existing third-party arrangements. However, it would also lead to a situation where financial entities would enter potential arrangements that would not come into effect, leading to minor additional costs for adding such arrangements to the register. Besides, such option is not covered under DORA's register and could create misalignment. Thus, Option C has not been retained.

Option D would ensure a comprehensive and systematic understanding of third-party arrangements, both under the Guidelines scope and DORA scope, for the competent authorities. The choice to merge the two registers still relies upon the financial entities if more efficient/for proportionality purposes.

Options B2 and D have been retained.

6) Guidelines on the assessment of risks and the criticality or importance of functions provided or supported by third-party service providers and their continued monitoring

Option A: the Guidelines would leave it up to financial entities to develop their own assessment framework.

Option B: the Guidelines would further specify, the approach for assessing the criticality or importance of functions.

Option C: the Guidelines would specify a framework for the ongoing monitoring of third-party arrangement.

Option A would not be effective, as it would not lead to the desired level of harmonisation of the assessment results.

Option B would ensure that there would be one harmonised framework but would provide additional criteria for the assessment of the impact of third-party arrangements. Assessing the operational risk impact is one aspect that is relevant for determining if a function is critical or important. A harmonised set of criteria to be implemented by financial entities would not create greater costs. Some of the criteria were applicable for the outsourcing framework and are still relevant.

Option C would ensure that changes to the criticality or importance of third-party arrangements would be identified by all financial entities. Under Option C, the Guidelines would provide a more specific framework for monitoring third-party risk. Option C would be effective. Additional costs would be limited to adjustments to the already existing risk management framework.

Options B and C have been retained.

7) Guidelines for competent authorities

Competent authorities already supervise third-party arrangements under the SREP Guidelines for institutions (see Article 97 of Directive 2013/36/EU), but also under Article 36 of Directive 2019/2034/EU (IFD), Article 9(3) of Directive (EU) 2015/2366, Article 5(5) of Directive 2009/110/EC and Article 35(3) of Regulation (EU) 2023/1114 (MiCAR).

Option A: the Guidelines should provide for a detailed procedural framework for supervision by competent authorities, the need to assess new critical and important functions provided by TPSPs before they are implemented.

Option B: the Guidelines should ensure that competent authorities are appropriately informed of any third-party arrangements but would leave the implementation of detailed supervisory procedures to the competent authority.

Assessment of third-party arrangements by competent authorities before their implementation (Option A) might lead to additional costs for financial entities, as the implementation of processes could be delayed. Competent authorities would need to have additional staff resources to ensure a timely assessment.

Option B is sufficient. However, given the periodicity of the SREP, additional information on new critical or important functions provided by TPSPs, while carrying low additional costs, ensures that competent authorities can effectively supervise financial entities and the concentration of third-party arrangements within the same TPSP.

Option B has been retained.

E. Cost-benefit analysis

The Guidelines impose a limited set of specific requirements on financial entities and competent authorities under the already existing framework, providing clarification and procedural guidance.

A higher level of clarity on third-party risk management benefits financial entities by creating a higher level of transparency regarding regulatory requirements and supervisory expectations.

Standardised requirements lead to a reduction in costs for implementing processes, in particular when assessed on a consolidated basis.

Harmonisation should increase the efficiency of supervision. In particular, the identification and supervision of third-party risks by competent authorities has a positive effect on the stability of the financial systems. However, this means that competent authorities will have to assign more resources to the supervision of such risk. Those costs should be limited, as, on a risk-based approach, such measures should be limited to critical or important and competent authorities are already familiar with framework.

The Guidelines aim to ensure that financial entities cannot become empty shells; this additional assurance protects the level playing field within the EU/EEA.

However, the Guidelines will trigger some implementation costs for financial entities, which will differ depending on their nature:

a. For initial addressees (ie. credit institutions and investment firms subject to the CRD, payment institutions and e-money institutions, and third-country branches, as defined in point 1 of Article 47(3) of Directive 2013/36/EU), a detailed framework already existed with the previous EBA Guidelines on outsourcing. Therefore, the additional costs triggered by the Guidelines should be low overall.

b. For new addressees (ie. Class 1 minus investment firms, Class 2 investment firms, ART issuers and creditors as defined in point (2) of Article 4 of MCD), considering that the sectoral directives already establish a set of requirements for outsourcing that is quite detailed, the additional costs should be very low.

An overview of costs and benefits is provided in Table 1 below.

Table 1. Costs and benefits

Stakeholders	Costs	Benefits
Credit institutions and investment firms subject to the CRD (already within scope)	Negligible additional costs, because already had to implement the previous Guidelines on outsourcing	Reduction in costs for implementing processes due to standardised requirements Reduction in ongoing costs for negotiating outsourcing arrangements with service providers due to a non-
Payment institutions and e-money institutions (already within scope)	Negligible additional costs, because already had to implement the previous Guidelines on outsourcing	

Third-country branches, as defined in point 1 of Article 47(3) of Directive 2013/36/EU	Negligible additional costs, because already had to implement the previous Guidelines on outsourcing	debateable set of contractual conditions to be agreed on. Level playing field across all entity types Proportionality, due to focus on critical or important outsourcing
Class 1 minus investment firms and Class 2 investment firms	Low additional costs (IFD internal governance requirements)	
ART issuers	Low additional costs (MICAR internal governance requirements)	
Creditors as defined in point (2) of Article 4 of MCD (only legal entities) which are financial institutions	Negligible to low costs, depending on the category above it falls into	
Third-party service providers (TPSPs)	Costs related to the reduction in flexibility of the contracts, due to supervisor demands	Transparency and clarification of their role with respect to the service provided to any FE
Competent authorities	Higher supervision costs due to increased scope of application of guidelines	Increased efficiency of supervision, due to increased harmonisation, and proportionality Protection of the level playing field Stability of the financial systems

5.2 Overview of questions for consultation

Question n. 1 for Public Consultation: Are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?

Question n. 2 for Public Consultation: Is Title II appropriate and sufficiently clear?

Question n. 3 for Public Consultation: Are Sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?

Question n. 4 for Public Consultation: Is Title IV of the Guidelines appropriate and sufficiently clear?

Question n. 5 for Public Consultation: Is Annex I, provided as a list of non-exhaustive examples, appropriate and sufficiently clear?

5.3 Feedback on the public consultation

[to be updated following the updates of the GL]

The EBA's update of the Guidelines

1. The EBA has taken into account and provided detailed feedback on the comments received during the public consultation. The following table provides a summary of the responses to the consultation and of the EBA's analysis.

2. Overall, the Guidelines have been reviewed to provide ….

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

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
General comments [			
Responses to questions in Consultation Paper EBA/CP/2025/xx			
Question 1.			
Question 2.			
Question 3.			