EBA/GL/2026/09

18 September 2026

Final report

EBA Guidelines

on the sound management of third-party risk regarding non-ICT services

1. 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 that financial entities continue to effectively strengthen their governance arrangements including their operational resilience.

Directive 2013/36/EU (Capital Requirements Directive – CRD) strengthens the governance requirements for institutions and Article 74(3) of the CRD gives the EBA the mandate to develop guidelines on institutions' governance arrangements. Operational resilience is an integral objective of the sound governance arrangements and effective internal control mechanisms required pursuant to Article 74 of Directive 2013/36/EU (CRD). Third-party risk management is one of the specific elements of institutions' governance arrangements. Directive 2019/2034/EU (Investment Firm Directive – 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 (Markets in Crypto-Assets Regulation – 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 (Markets in Financial Instruments Directive II – MiFID II) contains explicit provisions regarding the outsourcing to TPSPs of operational functions in the area of investment services and activities. Directive 2015/2366/EU (Payment Services Directive 2 – PSD 2) 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 (Digital Operational Resilience Act – DORA) also needs to be considered, since information and communication technology (ICT) services provided by TPSPs to financial entities are within DORA's scope of application. In this regard, to bridge the gap and to enable financial entities to have a holistic approach on third-party risk management, non-ICT services provided by TPSPs to support financial entities' functions are within the scope of these Guidelines with a particular focus on the ones supporting critical or important functions. 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 when they are used to

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

support 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 make sure that compliance with EU legislation and regulatory requirements (e.g. professional secrecy, access to information, protection of personal data) is ensured and that the competent authority is able to effectively supervise financial entities, in particular regarding critical or important functions supported by TPSPs.

The Guidelines provide a definition of critical or important functions that have a material impact on the financial entity's risk profile and is fully consistent with the definition under Regulation (EU) 2022/2554. If non-ICT services supporting critical or important functions are provided by TPSPs, stricter provisions apply to these third-party arrangements than to other third-party arrangements.

Competent authorities are required to effectively supervise financial entities' third-party arrangements with a particular focus on non-ICT services supporting critical or important functions provided by TPSPs, including identifying and monitoring concentration risk at individual level and assessing whether such concentration could pose a risk to the stability of the financial system. When carrying out this assessment, competent authorities should take into account the extent to which the same TPSPs are relied upon by other financial entities, where such information is available to them.

2. Background and rationale

1. Trust in the reliability of the financial system is crucial for its proper functioning and is a prerequisitefor its contribution to the broader economy. Effective internal governance arrangements are fundamental for credit institutions subject to Directive 2013/36/EU (CRD) ([2]), 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) ([3]), issuers of asset-referenced tokens (ARTs) subject to Regulation (EU) 2023/1114 (MiCAR) ([4]), payment institutions as defined in Article 4(4) of Directive (EU) 2015/2336 (PSD 2) ([5]) and electronic money institutions within the meaning of Directive 2009/110/EC (EMD) ([6]) (all together referred to as 'financial entities') and the financial system they form part of, to operate well.

2. Over the 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 group- or institutional protection scheme (IPS). 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 non-information and communication technology (non-ICT) services supporting important or critical function provided by TPSPs, in particular by the ones located outside the European Union, creates specific risks both for financial entities and for their competent authorities and should be subject to appropriate oversight. Any third-party arrangements, including outsourcing and subcontracting regarding 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's internal control functions or the ability of those financial entities and the competent authorities to oversee and supervise compliance with legal and regulatory requirements. The responsibility of the financial entity's management body and all its

[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 (OJ L 176, 27.6.2013, pp. 338–436, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

[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, pp. 1–63, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

[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, 9.6.2023, pp. 40–205, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

[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 (OJ L 337, 23.12.2015, pp. 35–127, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

[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 (OJ L 267, 10.10.2009, pp. 7–17, ELI: http://data.europa.eu/eli/dir/2009/110/oj).

activities can never be delegated to TPSPs. Thus, while those Guidelines apply for the management of third-party risk with regard to non-ICT services, DORA provides the framework for managing third-party risk associated with ICT services.

4. 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. In this context, third-country financial entities may seek to minimise the effective transfer 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. 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.

5. Functions that are considered critical under a resolution perspective may also rely on non-ICT services provided by TPSPs. Third-party arrangements should not create impediments to the resolvability of the financial entity where applicable.

6. Financial entities should be able to effectively control and challenge the quality and performance of non-ICT services supporting critical or important 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 non-ICT services supporting critical or important functions provided by TPSPs meet regulatory requirements.

7. 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 ([7])). For payment institutions, these Guidelines should be read in conjunction with, and without prejudice to, the relevant EBA Guidelines mandated under Directive 2015/2366/EU (PSD 2).

8. 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's size and internal organisation and the nature, scope and complexity of its activities.

Rationale and objective of the Guidelines

9. The EBA is updating its 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 taking into account the entry into force

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

of Regulation (EU) 2022/2554 (DORA). The scope of application of these Guidelines now covers institutions subject to Directive 2013/36/EU (CRD), creditors as defined in point (2) of Article 4 of Directive 2014/17/EU (MCD) which are financial 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 (IFR), payment and electronic money institutions (referred to as 'payment institutions') and issuers of ARTs subject to MiCAR. 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 PSD 2. 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.

10. The Guidelines take into account and are consistent with the current requirements under the Directive 2013/36/EU (CRD), Directive 2014/65/EU (MiFID II) ([8]), Directive 2019/2034/EU (IFD) ([9]), Directive 2009/110/EC (Electronic Money Directive – EMD), Directive (EU) 2015/2366 (PSD 2), Directive 2014/59/EU (Bank Recovery and Resolution Directive – BRRD) ([10]), 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 published by the Financial Stability Board (FSB) and the Basel Committee on Banking Supervision (BCBS), have been taken into account.

11. Under Article 16 of Regulation (EU) No 1093/2010 (the EBA Regulation) ([11]), the EBA is required to issue guidelines and recommendations addressed to competent authorities and financial institutions to establish consistent, efficient and effective supervisory practices and 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 services 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 achieved to ensure a level playing field, foster supervisory convergence and enable financial entities to have a holistic approach on third-party risk management.

12. 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

[8] 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, pp. 349–496, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

[9] 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 (OJ L314, 5.12.2019, pp. 64–114, ELI: http://data.europa.eu/eli/dir/2019/2034/oj).

[10] 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, pp. 190–348, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

[11] 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, pp. 12–47, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

adequately and effectively supervise TPSPs supporting EU financial entities' critical or important functions.

13. 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 ([12]). 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 same approach exists under Directive 2009/138/EC (Solvency II) ([13]), while, in the context of outsourcing, the PSD 2 uses 'important function' for the purpose of identifying functions under outsourcing arrangements for which specific requirements apply.

14. Article 109(2) of the 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 of the CRD or Article 109(1) of the CRD in conjunction with Article 7 of Regulation (EU) No 575/2013 (Capital Requirements Regulation – CRR) ([14]). 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 electronic money institutions, issuers of ARTs, investment firms, as well as firms subject to Directive 2011/61/EU ([15]) and Directive 2009/65/EC ([16])) in a consistent and well-integrated way but also taking into account sectoral specific requirements that apply on an individual basis.

Governance of third-party arrangements

15. Institutions, in accordance with Article 74 of the CRD, payment institutions in line with Article 11 of PSD 2, 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 effective processes to identify, manage, monitor and report the risks they are or might be exposed

[12] 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, pp. 1–83, ELI: http://data.europa.eu/eli/reg_del/2017/565/oj).

[13] 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 (OJ L 335, 17.12.2009, pp. 1–155, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

[14] 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, pp. 1–337, ELI: http://data.europa.eu/eli/reg/2013/575/oj).

[15] 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 (OJ L 174, 1.7.2011, pp. 1–73, ELI: http://data.europa.eu/eli/dir/2011/61/oj).

[16] 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) (OJ L 302, 17.11.2009, pp. 32–96, ELI: http://data.europa.eu/eli/dir/2009/65/oj).

to. In this regard, the Guidelines include third-party risk management 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 the contractual arrangement regarding the use of non-ICT services supporting critical or important functions provided by TPSPs;

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 on non-ICT services supporting functions that are provided by TPSPs.

16. Financial entities must define criteria or establish a methodology to determine whether the function to be supported by a TPSP is considered critical or important. Arrangements with TPSPs supporting critical and important functions can have a material impact on the financial entities' risk profile. To this end, more stringent provisions apply to the arrangements with TPSPs supporting financial entities' critical or important functions to ensure the soundness of their governance arrangements and that competent authorities can exercise effective supervision.

17. The risks to be considered include those associated with the financial entities' relationship with the TPSP, the risks caused by allowing subcontracting supporting critical or important functions, the concentration risk posed by multiple arrangements with the same TPSP and/or the concentration risk posed by a limited number of TPSPs or with closely connected TPSPs supporting critical or important functions. 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 TPSP supporting critical or important functions 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.

18. Similarly, arrangements with TPSPs supporting critical or important functions including 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.

19. Each form of third-party arrangement has its specific risks and advantages. Without prejudice to the waivers included in Article 21 of the CRD that may be granted when the conditions under Article 10 of the CRR are met and waivers under Article 109(1) of the CRD that apply when the

derogation under Article 7 of the 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.

20. If financial entities intend to use entities within the group to provide non-ICT services supporting 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 – including the financial conditions – are taken objectively. Financial entities should also ensure that they explicitly manage any 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 to, among other aspects, implement efficient processes at group level.

21. The same aspects that are relevant for third-party arrangements within a group also apply when institutions that are members of an institutional protection scheme use a central service provider to provide functions.

22. Arrangement with TPSPs supporting critical or important functions 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.

23. Financial entities should, in all instances, have robust governance arrangements in place for third-party arrangements that are not considered critical or important taking into account a risk-based approach and the application of the proportionality principle.

24. 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 ESG risks and consider the impact of their third-party arrangements on all stakeholders. Such aspects are of particular relevance when TPSPs are located in third countries.

25. 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. In particular, increased reliance on TPSPs supporting 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.

26. 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.

27. Arrangements with TPSPs supporting critical or important functions 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 rely on a TPSP to support a critical or important function should not in any way impede the resolvability of the institution.

28. The financial entities and competent authorities', including resolution authorities, right to audit, inspect, and access information, accounts and premises should be ensured within each written third-party agreement. Financial entities and competent authorities right to audit is key for providing the appropriate assurance that at least critical or important functions provided by TPSPs are provided as contractually agreed and in line with legal and regulatory requirements. To ensure that credit institutions can be effectively supervised, competent authorities must be granted explicit audit and access rights across all outsourcing and TPSP arrangements supporting critical or important functions. 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 financial entities are not to be considered 'third-party arrangements' under the scope of these guidelines.

29. The third-party agreement should specify whether subcontracting of critical or important functions, or material parts thereof, is permitted. Hence, the Guidelines further specify the conditions for subcontracting by the financial entities in the case of critical or important functions supported by TPSPs. Financial entities should always have the right to terminate the contract if planned changes to critical or important functions, including such changes caused by subcontracting, would have an adverse effect on the critical or important functions supported.

Supervision and concentration risks

30. 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 line with these guidelines. 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.

31. Competent authorities need to identify the concentration of third-party arrangements by TPSPs. The concentration of third-party arrangements with TPSPs regarding critical or important functions may lead to the disruption of the provision of financial services by multiple financial entities if the non-ICT service fails. 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.

3. Guidelines

EBA/GL/2026/09

18 September 2026

Guidelines on the sound management of third-party risk related to non-ICT services

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 ([17]). 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. The Guidelines set out the EBA's view on appropriate supervisory practices within the European System of Financial Supervision, or on 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 the 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).

[17] 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, pp. 12–47, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

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 (IFR) ([18]), 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 (Mortgage Credit Directive – MCD) ([19]) which are financial institutions should implement when they rely on third-party service providers (TPSPs) to provide non-ICT services supporting ([20]) functions with a particular focus on critical or important functions. These Guidelines apply to non-ICT services (hereafter 'services') provided by TPSPs, other than those within the scope of Chapter V of Regulation (EU) 2022/2554 (DORA).

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) ([21]), Article 9(3) of Directive (EU) 2015/2366 (PSD 2), Article 5(5) of Directive 2009/110/EC (EMD) ([22]) and Article 35(3) of Regulation (EU) 2023/1114 (MiCAR) ([23]), thereby fulfilling the competent authorities' duty to monitor the addressed entities' continuous compliance with the conditions of their authorization .

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 (DORA) ([24]) are excluded from the scope of application of these Guidelines, as they fall within the scope of DORA. In this regard, these Guidelines only cover the use of TPSPs that do not

[18] 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, pp. 1–63, ELI: http://data.europa.eu/eli/reg/2019/2033/oj).

[19] 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 60, 28.2.2014, pp. 34–85, ELI: http://data.europa.eu/eli/dir/2014/17/oj).

[20] The wording 'support' by TPSPs may include the provision of the full function within the meaning of these guidelines.

[21] 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 (OJ L 314, 5.12.2019, pp. 64–114, ELI: http://data.europa.eu/eli/dir/2019/2034/oj).

[22] 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 (OJ L 267, 10.10.2009, pp. 7–17, ELI: http://data.europa.eu/eli/dir/2009/110/oj).

[23] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 9.6.2023, pp. 40–205, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

[24] 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, pp. 1-79, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

provide ICT services supporting critical or important functions under DORA. Consistency has been ensured with DORA and its relevant mandates; while DORA sets out the framework on the management of third-party risks with regard to ICT services, these Guidelines apply to the management of third-party risks with regard to non-ICT services. However financial entities should have a holistic approach covering the management of third-party risk with regard to both ICT and non-ICT services provided by third party service providers.

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, 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 and, 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 (MCD) ([25]) 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. For EU branches of third country credit institutions (third country branches) within the meaning of Article 47 of Directive 2013/36/EU, these Guidelines should be read in conjunction with the EBA Guidelines on internal governance under Directive 2013/36/EU. As third-country branches do not have the legal personality and are not considered as separate legal entities from their head undertaking in the third country, a proportionate approach is appropriate for the application of these Guidelines. In this regard, while a written contract between the head undertaking and its EU branch is not possible as they are not legally distinct, the EU branch should have any other arrangement (such as service level arrangement or policies) to formally document the services required by the branch and performed by the head undertaking to enable the branch to comply with these guideline taking into account its specific nature.

[25] 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 60, 28.2.2014, pp. 34–85, ELI: http://data.europa.eu/eli/dir/2014/17/oj).

11. 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.

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

Scope of application

13. Without prejudice to Directive 2014/65/EU ([26]) and Commission Delegated Regulation (EU) 2017/565 ([27]) 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 2013/36/EU, Class 1 minus ([28]) and Class 2 ([29]) 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.

14. 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.

15. 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 ([30]).

[26] 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, pp. 349–496, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

[27] 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, pp. 1–83, ELI: http://data.europa.eu/eli/reg_del/2017/565/oj).

[28] 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.

[29] 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.

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

Definitions

16. 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 ([31]), the EBA Guidelines on internal governance under Directive (EU) 2019/2034 ([32]) and the EBA Guidelines on the minimum content of the governance arrangements for issuers of asset-referenced tokens under Regulation (EU) 2023/1114 ([33]) have the same meaning in these Guidelines.

17. In addition, for the purposes of these Guidelines, the following definitions apply:

Third-party arrangement	means an arrangement ([34]) of any form between a financial entity and a third-party service provider, including intragroup third-party service providers, for the support of one or more functions to the financial entity on a recurrent basis or an ongoing basis. 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 services supporting a function provided by third-party service providers or by subcontractors of the latter. The service by the third-party service provider may include 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 ([35])	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,

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

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

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

[34] 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).

[35] The wording 'critical or important function' is used only for the purpose of these Guidelines and is not the same 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).

	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 has entered into an arrangement with another service provider to further transfer a function ([36]), in whole or in part.
Third-party service provider	means an undertaking providing a service supporting a function under an arrangement with a financial entity.
Intragroup 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.
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.

[36] 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 n^{th} party service providers.

3. Implementation

Date of application

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

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

Transitional provisions

20. Where the review and the documentation of third-party arrangements supporting critical or important functions are not finalised by [date: two 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.

21. Regarding third-party arrangements supporting non-critical or important functions, their review and documentation might be done solely in the occasion of the renewal of such arrangements.

Repeal

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

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

Title I – Proportionality: group application and institutional protection schemes

1 Proportionality

23. 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.

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

25. When applying the principle of proportionality, financial entities ([37]) 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

26. 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 ([38]). For this purpose, the EU parent undertaking or the parent undertaking in a Member State should ensure that internal governance arrangements, processes and

[37] Payment institutions should also refer to the EBA Guidelines under PSD 2 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.

[38] 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.

27. Where applicable, financial entities, in accordance with paragraph 26, 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 group or institutional protection scheme (IPS) ([39]), 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 institutional protection scheme (IPS), 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.

28. In addition to paragraph 27, 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 services supporting 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 services supporting 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 services supporting critical or important functions provided, including a summary of the risk analysis, including legal risks,

[39] In accordance with Article 113(7) of the 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.

compliance with 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 the group or the institutional protection scheme (IPS), 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 within the group or institutional protection scheme;

e. where those financial entities rely on an exit plan, as referred to in Section 14, for third party arrangement supporting 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.

29. 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.

30. 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 risk

31. As part of the overall internal control framework including internal control mechanisms, financial entities should have a holistic risk management framework extending across all business lines and internal units. Under that framework, financial entities should establish whether an arrangement with a TPSP falls under the definition of third-party arrangement provided in these Guidelines. Under this assessment, consideration should be given to:

a. determine whether the services they rely or plan to rely on are non-ICT services;

b. whether the TPSP is providing non-ICT services supporting a function at least on a recurrent or ongoing basis; and

c. whether the function under b) is critical or important.

32. Where an arrangement with a TPSP covers multiple functions, 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. 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 an ICT service is material for the provision of the services under the third-party arrangement and thus triggers the application of DORA framework ([40]).

33. As a general principle, the following services are excluded from the scope of application of these Guidelines ([41]):

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

b. a regulated financial service that is legally required to be performed by another financial entity regulated under Union law including by financial entities not in the scope of these guidelines but regulated under financial services Union law (e.g. custody and safekeeping services, trading venues including regulated market, multilateral trading facilities…);

c. market information services;

d. financial services transactions between financial institutions as counterparties (e.g. inter-bank lending); financial transaction with central banks (e.g. deposit and lending facilities);

e. Payment network infrastructures (e.g. Visa, MasterCard, European payment initiatives, WERO, GIE CB);

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

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

b. correspondent banking services;

c. 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, printing

[40] See also ESAs Q&A30.

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

services, providing legal opinion including on tax , and representation in front of the court and administrative bodies, public relation consulting, cleaning, gardening and maintenance of the institution's or payment institution's premises, medical services, servicing of company cars, catering, canteen, cafeteria, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators); the acquisition of goods (e.g. plastic cards, card readers, office supplies, personal computers, furniture…) or the acquisition of utilities (e.g. electricity, gas, water, telephone services).

4 Critical or important functions

34. Financial entities should always consider a function as critical or important in the following situations ([42]), where its disruption, discontinuity, defect or failure in its performance would materially impair:

    a. their continuing compliance 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.

35. 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.

36. 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 ([43]) by a competent authority, they should automatically consider such function as critical or important, as referred to in Section 1211.1.

37. In the case of financial entities that are subject to Directive 2014/59/EU ([44]), 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

[42] See also Article 30 of the 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.

[43]

http://data.europa.eu/eli/reg/2023/1114/oj

[44] 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, pp. 190–348, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

as defined in Article 2(1), points (35) and (36) of Directive 2014/59/EU and using the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778 ([45]). Functions that are necessary to perform activities of core business lines or critical functions should be considered 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 a material impact on the operational continuity of the core business lines or critical functions.

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, which should include a policy on third-party risk management as referred to in Section 6 which should complement financial entities operational risk management and supports its operational resilience. The policy should allow for the implementation of a holistic approach to third-party risk management. Financial entities should have the flexibility to develop either integrated or separate strategies regarding ICT and non-ICT third-party risk management. The management body should ensure, on the basis of an assessment of the overall risk profile of the financial entity, and taking into account the principle of proportionality, that the financial entity itself regularly reviews the risks identified in respect to third-party arrangements on the use of services supporting critical or important functions.

39. The overall internal control framework, including the risk management framework, should enable financial entities to make well-informed decisions on risk-taking and ensure that risk management measures are appropriately implemented.

40. Taking into account the application of the principle of proportionality as referred to in Title I, financial entities should identify, assess, monitor, and manage all risks resulting from arrangements with TPSPs to which they are or might be exposed in accordance with Section 1211.2. Financial entities should also ensure that they comply with all requirements under Regulation (EU) 2016/679, including for their third-party arrangements.

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

[45] 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, pp. 41–47, ELI: http://data.europa.eu/eli/reg_del/2016/778/oj).

42. 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. ensuring the internal organisation of the financial entity;

    c. approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential 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. exercising 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.

43. 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, appropriately skilled resources to ensure appropriate management and monitoring of third-party arrangements.

44. 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 the application of proportionality under 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 ([46]). 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.

45. 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 ([47]) at all times, including the management body effectively carrying out its responsibilities as set out in paragraph 42 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 (including 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 third-party arrangement supporting critical or important functions by a TPSP; and

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

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

    a. they can take and implement decisions related to their business activities and their critical or important functions;

    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 regarding data and other information are in place;

[46] 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.

[47] 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 (PSD 2) 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 PSD 2).

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

f. with regard to the third-party arrangements supporting critical or important functions, 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 the contractual arrangement regarding the use of non-ICT services supporting critical or important functions provided by TPSP

47. The management body of a financial entity[48] that has third-party arrangements in place or plans on entering into such arrangements should approve a written policy on the use of non-ICT related services supporting critical or important functions provided by TPSP. The management body should review it at least once a year and, update it where relevant. Changes made to the policy should be implemented in a timely manner and as soon as it is possible within the relevant contractual arrangements. The management body should also ensure the policy's implementation, as applicable, on an individual, sub-consolidated, and consolidated basis.

48. The policy should include the main phases of the life cycle for the adoption and use of contractual arrangements with TPSP. It should cover, for each main phase of the life cycle of the contractual arrangement, at least:

a. the responsibilities of the management body in line with paragraphs 38 and 42, including its involvement, as appropriate, in the decision-making on the use of services supporting critical or important functions provided by TPSP;

b. the involvement of business lines, internal control functions, and other individuals in respect of contractual arrangements supporting critical or important functions;

c. the identification of the role or member of senior management responsible for monitoring the relevant contractual arrangements, specifying how that role or member of senior management shall cooperate with the internal control functions, unless it is

[48] 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.

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;

d. the planning of contractual 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 1211.2;

   v. due diligence checks on prospective TPSPs, including the measures required under Section 1211.3;

   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;

e. the implementation, monitoring, and management of third-party arrangements supporting critical or important functions, 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, where applicable;

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

g. the exit strategies and termination processes, including a requirement for a documented exit plan for non-ICT services supporting critical or important function to be provided by TPSPs, in accordance with Section 14.

49. The policy may be merged with the policy foreseen under Article 28(10) of DORA ([49]). However, it should differentiate between the following:

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

    b. non-ICT services supporting critical or important functions provided by TPSPs that are authorised by a competent authority and those that are not;

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

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

50. Financial entities should ensure that the policy covers the identification of potential impact on the following areas resulting from 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 manage the risks;

    c. the business continuity measures; and

    d. the performance of their business activities.

7 Conflicts of interests

51. Financial entities ([50]) should identify, assess, and manage conflicts of interests with regard to their third-party arrangements.

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

53. When services supporting critical or important 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, the conditions, including the financial conditions, are to be taken objectively. However, the pricing of service synergies resulting from providing the same or similar services to several

[49] Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (OJ L, 2024/1773, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1773/oj).

[50] 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.

institutions within a group- or an institutional protection scheme (IPS) 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

54. Financial entities ([51]) should have in place, maintain, and periodically test appropriate business continuity plans with the aim to ensure the continuity of the financial entity's 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 (IPS)- related structure may rely on centrally established and periodically tested business continuity plans regarding their functions provided by TPSPs, in accordance with Section 2.

55. Business continuity plans should take into account the possible event of a failure or disruption at a TPSP impacting the provision of critical or important functions. Taking into account the application of proportionality, as part of the overall business continuity policy, financial entities should conduct a business impact analysis (BIA) of their exposures to severe business disruptions. Under the BIA, financial entities should assess the potential impact of severe business disruptions by means of quantitative and qualitative criteria, using internal and external data and scenario analysis, as appropriate. The BIA should consider the criticality of identified and mapped business functions, support processes, third-party dependencies, and substitutability of the TPSP.

9 Internal audit function

56. The activities of the internal audit function ([52]), 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 ([53]) and programme should include the third-party arrangements supporting 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

[51] 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.

[52] 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 PSD 2 (Guidelines on authorisation and registration under PSD 2).

[53] 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.

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.

57. 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

58. As part of their risk management framework, financial entities should maintain an updated register of information on all third-party arrangements that are within the scope of these guidelines, 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 supporting critical or important functions and other third-party arrangements. Where direct TPSPs of financial entities provide non-ICT services and said TPSPs use ICT subcontractors effectively underpinning such non-ICT services supporting critical or important functions as defined under Regulation (EU) 2022/2554, those should be documented in the register in line with the present guidelines.

59. Financial entities should also maintain the documentation of ended third-party arrangements within the register and the supporting documentation for an appropriate period.

60. Taking into account the application of proportionality as referred to in Title I of the Guidelines, and under the conditions set out in paragraph 28(d), financial entities within a group, institutions permanently affiliated to a central body, or financial entities that are members of the same institutional protection scheme may keep the register centrally and collect the information at the highest level of consolidation.

61. Taking into account the application of proportionality under Title I of the Guidelines, the register should be consistent to the extent possible, with the register of information under Article 28(3) of DORA. Financial entities are encouraged to avoid any discrepancies between those two registers. Financial entities also have the possibility to combine both in one single register. The register for the non-ICT services 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;

c. where applicable, the financial entities within the scope of the prudential consolidation or institutional protection scheme, that make use of the TPSPs, in accordance with paragraph 60;

d. whether or not the TPSP or subcontractor is part of the group or a member of the institutional protection scheme (IPS) 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. whether or not (yes/no) the non-ICT service provided by a TPSP is supporting a critical or important function, including, where applicable, a brief summary of the reasons why the function is considered critical or important

g. a category assigned by the financial entity that reflects the nature of the functions covered by the third-party arrangement as described within the financial entity's own internal categorisation. If an arrangement covers multiple functions, then the financial entity should report as many categories as the functions provided;

h. the name of the TPSP, an identifier (LEI, EUID for legal persons or other alternative identifiers), the corporate registration number, the registered address and other relevant contact details, and the name of its ultimate parent company and an identifier (if any);

i. the country or countries where critical or important function is to be performed;

62. For third-party arrangements supporting critical or important functions, 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 subcontracted, including the country where the subcontractors are registered, an identifier (LEI, EUID, or legal persons or other alternative identifiers), the type of functions or material part subcontracted, the rank in the chain, the location from where the non-ICT related 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. the identification of alternative TPSPs, where possible, in line with paragraph 61 point (g);

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

63. Financial entities should, upon request, make available to the competent authority either the full register of all existing third-party arrangements ([54]) or sections specified thereof. Financial entities should provide this information in a processable electronic form and may use the same format set out under the DORA ITS (e.g. a commonly used database format, comma separated values).

64. 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. The information, where applicable, can be made available at consolidated or sub-consolidated level.

65. Financial entities, 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 61 and 62.

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

67. 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).

[54] 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.

Title IV – Third-party arrangement process

11 Pre-contractual analysis

68. 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 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; and

    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

69. Financial entities should ensure that the use of TPSPs to provide functions of banking activities or payment services, the 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 different Member State or a third country 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.

70. Without prejudice of the requirements established under Article 32 of the Commission Delegated Regulation (EU) 2017/565, financial entities should ensure that the use of TPSPs in a third country for the provision of functions of banking activities or payment services or the issuance of ARTs as defined in Article 3(1), point (6) of Regulation (EU) 2023/1114, to an extent that the performance of that function would require authorisation or registration by a competent authority in the Member State where the financial entity is authorised, 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) ensures that the competent authorities are able, at least, to:

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 (EU) 2019/2034, 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 (EU) 2019/2034, 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

71. Financial entities should consider, on a risk-based approach, the potential impact of third-party arrangements on 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.

72. Financial entities should consider:

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

i. identify, monitor and manage relevant 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 ([55]).

73. The risk assessment should include, where appropriate or relevant, 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, considering the application of the principle of proportionality referred to in Title I, should document the analysis performed and its results and should estimate the extent to which the arrangement would increase or decrease their risk level. Taking into account the application of the principle of proportionality under 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.

74. Within the risk assessment, financial entities should also consider 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:

[55] 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) (OJ L 119, 4.5.2016, pp. 1–88, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

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;

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.

75. Where a third-party arrangement supporting critical or important functions 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.

76. 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,

b. 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;

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

d. 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;

e. 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

77. Before entering into third-party arrangements and considering all the relevant risks related to the non-ICT services 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.

78. 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, 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.

79. With regard to critical and important functions ([56]), financial entities should ensure that the TPSP has:

a. the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources 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;

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

c. geographic dependencies and manage the 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;

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.

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

81. 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.

82. Financial entities should take appropriate steps to ensure that TPSPs act in a manner consistent with their values and code of conduct. With regard to TPSPs located in third countries and, if applicable, their subcontractors, financial entities should be satisfied that such TPSPs act 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 including the prohibition of child labour and, environmental protection

12 Contractual phase

83. The rights and obligations of the financial entity and the TPSP should be clearly allocated and set out in written contract.

84. The contractual arrangement should include at least the following elements:

a. a clear and complete description of non-ICT services supporting 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 1312.1 that 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 changing the location(s);

c. the governing law of the contract;

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

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

f. provisions on ensuring that the data that are owned by the financial entity can be easily 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;

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

h. 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;

i. termination rights and related notice periods for the termination of the third-party arrangement, as specified in Section 1312.3;

j. 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.

85. In addition to the elements referred to in paragraph 84, the third-party arrangement supporting critical or important functions should set out at least:

a. the agreed service level descriptions, including updates and revisions thereof, with precise quantitative or/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 provide the services supporting critical or important functions 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 out 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 access of financial entities and competent authorities to inspect and audit the TPSP, as specified in Section 1312.2;

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, establishing 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 ensuring 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.

86. Without prejudice to the requirements set out under 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

87. The third-party arrangements on the use of services supporting critical or important function by TPSPs should specify whether the 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 supporting critical or important functions by TPSPs cannot reduce the ultimate responsibility of the financial entities' management body 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. Among those subcontractors that provide services supporting critical or important functions, financial entities should notably focus continuously on those subcontractors that effectively underpin the non-ICT related service supporting a critical or important functions.

88. If the subcontracting of services supporting critical or important functions or material parts thereof is permitted, financial entities should determine whether the subcontractor effectively underpins the non-ICT related service that supports the critical or important function, and, if it does, record it in the register.

89. If the use of subcontractors supporting critical or important functions or material parts thereof is permitted, the written agreement between the financial entity and the TPSP 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 and manage all risks associated with the location of the current or potential subcontractors, and their parent company, and with the location where the service concerned is provided from;

    d. that the TPSP is obliged to monitor those functions that it has subcontracted 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 supporting critical or important functions;

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

    g. that the TPSP has to ensure the continuity of the provision 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 grants 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 changes to written agreements between the financial entity and the TPSP that are necessary to comply with EU legal requirements and the specifications provided in these Guidelines, should be implemented in a timely manner and as soon as it is possible by the subcontractor;

    j. the financial entity should document and communicate the planned timeline for the implementation of such changes.

90. The written agreement between the financial entities and the TPSPs should specify that the TPSP should notify the financial entity about new subcontracting arrangements and 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 new subcontracting arrangements or such material changes might affect the ability of the TPSP to meet its contractual obligations *vis-a-vis* the financial entity.

91. The written agreement should include a reasonable notice period by which the financial entity is able to approve or to object to new subcontracting arrangements or changes of such arrangements.

92. The TPSP should only enter into new subcontracting arrangements or implement 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.

93. Where the financial entity is of the opinion that the new subcontracting arrangement or the material changes referred to in paragraph 90 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 new subcontracting arrangement or to the changes and request modifications to the subcontracting arrangement or to those changes before they are entered into or implemented.

94. Financial entities should ensure that the TPSP appropriately identifies all subcontractors and monitors the subcontractors providing critical or important functions or material parts thereof that with a particular focus on subcontractors effectively underpinning the non-ICT related service supporting a critical or important function.

95. The financial entity should ensure in the written agreement with the TPSP that the agreement between the TPSP and the subcontractor may be terminated in each of the following cases:

— the financial entity has objected to a new subcontracting arrangement supporting critical or important functions or to material changes to the subcontracting arrangements supporting critical or important functions and requested for modifications to those arrangements, but the TPSP has nevertheless entered into the new subcontracting arrangement or implemented those material changes;

— the TPSP has entered into a new subcontracting arrangement supporting critical or important functions or 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 service supporting 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

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

97. Regardless of the criticality or importance of the function performed by TPSPs, the written contractual 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 in third countries.

98. With regard to contractual arrangements supporting critical or important functions, financial entities should ensure 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. access to all relevant business premises (e.g. head offices and operational centres), as well as the right to take copies of relevant information and documentation if they are critical to the operations of the TPSP ('access and information rights'); 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.

99. For services not supporting critical or important functions provided by TPSPs, financial entities should consider including the access and audit rights as set out in paragraph 998 (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.

100. Financial entities should ensure that the contractual arrangement does not impede or limit the effective exercise of access, information, and audit rights by them, competent authorities or third parties appointed by the financial entity or competent authorities to exercise such rights.

101. 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 ([57]).

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

[57] 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; and

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

103. For services supporting critical or important functions provided by TPSPs financial entities should assess:

a. whether third-party certifications and third-party or internal audit reports as referred to in paragraph 102(b) are adequate and sufficient to comply with their regulatory obligations. Financial entities should not rely solely on these certifications and reports over time.

b. when relying on pooled audits as referred to in paragraph 102(a), whether they have sufficient information and are sufficiently involved in scoping, planning, performing and reporting the audit and its findings.

104. Financial entities should make use of the method referred to in paragraph 102(b) only if they:

a. are satisfied with the audit plan for the services 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 to support critical or important functions.

105. Before a planned onsite 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.

106. 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.

107. Where the third-party arrangement carries a high level of 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

108. The financial entity should be able to terminate the third-party arrangements, in accordance with applicable law, including in the following situations:

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

b. where circumstances identified throughout the monitoring that are deemed capable of altering the performance of the service provided, including material changes that affect the arrangement or the situation of the 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 evidenced weaknesses pertaining to its risk management and security of confidential, personal or otherwise sensitive data, or non-personal data;

e. where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement.

109. The third-party arrangement should facilitate the transfer of the services supporting a critical or important 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 services supporting a critical or important 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 services supporting a critical or important function 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 services supporting a critical or important function in the event of the termination of the third-party arrangement.

13 Monitoring

110. Following a risk-based approach, financial entities should monitor the performance of the TPSPs providing services with regard to third-party arrangements and monitor on an ongoing basis the third-party arrangements supporting critical or important functions consistently with paragraph 112. 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 supporting critical or important functions. Where the risk, nature or scale of a function has materially changed, financial entities should reassess the criticality or importance of that function in line with Section 4.

111. Financial entities should monitor and manage their internal concentration risks caused by third-party arrangements, including with regard to the use of subcontractors for supporting critical or important functions, taking into account Section 11.2 of these Guidelines.

112. Financial entities should ensure, on an ongoing basis, that third-party arrangements supporting 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-certifications, and independent reviews; and

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

113. Financial entities should take appropriate measures if they identify actual or potential shortcomings in the performance of the services provided by a TPSP. If shortcomings are identified, financial entities should take appropriate corrective or remedial actions or terminate the contract.

14 Exit strategies regarding third-party arrangement supporting critical or important functions

114. Financial entities should have a documented exit strategy when services supporting critical or important functions are provided by TPSPs, which is in line with their strategy on third-party risk management and business continuity plans ([58]), taking into account at least the possibility of:

a. the termination of third-party arrangements;

b. the failure of the TPSP;

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

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 performance of the function;

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

115. Financial entities should ensure that they are able to exit third-party arrangements supporting critical or important functions performed by TPSPs without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their provision of services to clients. To achieve this, they should:

a. develop and implement exit plans that are realistic, feasible, and 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.

[58] 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.

116. When developing exit strategies for third-party arrangements supporting critical or important functions, financial entities should:

a. take into account the results of the analysis described in paragraph 73;

b. define the objectives of the exit strategy;

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

d. define success criteria for the transition of services provided by TPSPs and the data held by them; and

e. 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 or other appropriate actions.

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

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

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

119. 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 onsite inspections.

120. 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 supporting critical or important functions, such as:

a. the detailed risk analysis;

b. information on 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 a disruption to the provision of the services; and

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

121. 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.

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

a. whether financial entities monitor and manage appropriately third-party arrangements, in particular those supporting critical or important functions;

b. whether financial entities have sufficient resources in place to monitor and manage third-party arrangements supporting critical or important functions;

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.

123. 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.

124. Within their assessment, competent authorities should take into account all risks, in particular ([59]):

a. 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;

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

[59] 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.

f. the extent to which the financial entity controls the TPSP or has the ability to influence its actions, and 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.

125. 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 of new potentially critical functions ([60]) that have been identified during this assessment.

126. 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 non-ICT services supporting critical or important functions provided by TPSPs or requiring exit from one or more third-party arrangements. Considering 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.

127. Competent authorities should be satisfied that they are able to perform effective supervision, particularly when services supporting critical or important functions for financial entities are provided by TPSPs and undertaken outside the EU/EEA.

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

[60] As defined under Article 2(1), point (35) of the BRRD.

4. Accompanying documents

4.1 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 are 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), and 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 ([61]) and the BCBS work on third-party risk management published in December 2025 ([62]).

B. Policy objectives

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

[62] See: BCBS Principles for the sound management of third-party risk, published in December 2025: Principles for the sound management of third-party risk.

To ensure a level playing field and to meet the requirements under CRD, IFD, MiFID II, PSD 2, EMD, and MiCAR, and to take into account the entry into force of DORA, the EBA is now updating the Guidelines on outsourcing issued in 2019 to establish one common holistic framework for the management of third-party risk regarding non-ICT services by all financial institutions within the scope of the EBA's action. This update bridges the gap with Regulation (EU) 2022/2554, which regulates the use of third-party service providers for ICT-related services. Therefore, the use of ICT third-party service providers providing ICT services, including when supporting critical or important functions, has been excluded from the scope of application of these Guidelines.

The link between the existing outsourcing framework as a subset of the third-party risk management framework has been clarified and continues to exist.

In line with the principle of proportionality and a risk-based approach, the Guidelines focus on those non-ICT services that are supporting critical or important functions and are provided by third-party service providers (TPSPs) to financial entities. While financial entities must manage all their risks, the guidelines specify stricter provisions to manage the risks of non-ICT third-party arrangements that concern critical or important functions compared with other third-party arrangements that concern non-ICT functions that are not deemed critical or important.

The Guidelines aim to clarify the supervisory expectations regarding the management of third-party risks, including towards third-party service providers located in third countries to ensure that third-party arrangements are concluded and monitored appropriately.

The Guidelines aim to ensure that competent authorities are able to identify concentration risks 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) of the CRD mandates the EBA 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. Article 76 of the CRD sets out requirements for the involvement of the management body in risk management and Article 88 of the 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 the internal governance of investment firms which are not small and interconnected under Article 12(1) of Regulation (EU) 2019/2033 and gives the EBA, in consultation with ESMA, the mandate to issue guidelines in this area ([63]) while Regulation (EU) 2023/1114 (MiCAR) sets out a specific mandate for the EBA, in consultation with ESMA and the ECB, to develop guidelines on internal governance regarding issuers of ARTs. Directive 2014/65/EU (MiFID II) also contains explicit provisions regarding the outsourcing of operational functions in the field of investment services and activities. Directive (EU) 2015/2366 (PSD 2) sets out requirements for the outsourcing of functions by payment institutions.

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

Financial entities must ensure that sensitive data, including personal data, are adequately protected and kept confidential. Financial entities must comply with 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).

All of the above forms the baseline scenario of the impact assessment, which focuses only on the 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 (i.e. credit institutions and investment firms subject to CRD, payment institutions (PIs) under PSD 2, 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, creditors as defined in point (2) of Article 4 of Directive 2014/17/EU (MCD) which are financial institutions, and issuers of ARTs, taking into account the application of the principle of proportionality.

Institutions under CRD (i.e. credit institutions and investment firms) will continue to be subject to the GLs as they are required under Article 74 of the 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 PSD 2, 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 with unlevel playing field between investment firms within CRD's scope and the others within IFD's scope, or ARTs issuers within CRD's scope. In particular, those financial entities would need to implement arrangements under a different framework for the different types of activities they perform using third-party service providers.

Furthermore, while all investment firms are subject to MiFID, which sets out requirements on outsourcing, a prudential framework for investment firms was introduced in 2019 with Directive (EU) 2019/2034 (IFD). In accordance with this framework, Class 2 investment firms are covered by IFD provisions requiring them to have sound governance arrangements (Article 26 of the IFD) and should therefore be covered by the GLs ensuring a level playing field. 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 as Article 26 of the IFD does not apply to them.

Directive 2014/17/EU (MCD) defines non-credit institutions as '*any creditor that is not a credit institution*' (Article 4, point (10) of the 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 their trade, business, or profession (Article 4, point (2) of the MCD). Even if there are no provisions regarding governance or outsourcing arrangements under the MCD, creditors that are financial

institutions are in any case included in the specific section on outsourcing of the EBA GL on arrears and foreclosure.

Following the entry into force of Regulation (EU) 2023/1114 (MiCAR), issuers of ARTs that are not credit institutions 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 of the Guidelines. Moreover, issuers of ARTs are subject to requirements on 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 update their critical or important third-party arrangements (TPAs), set up or update the register of TPAs regarding non-ICT services in line with the guidelines.

Option B1: setting a fixed transitional period of two years to review critical or important TPAs and complete or update the register.

Option B2: setting a period of two years to review critical or important TPAs. Where not possible, financial entities should liaise with their competent authorities. For TPAs that are not critical or important, no timeline is foreseen but an update on the date of the renewal.

All options would be effective in achieving the desired prudential outcome of having all third-party arrangements documented in a way that differentiates between critical and important functions, setting out a framework for such third-party arrangements, and for establishing a complete register to be submitted to competent authorities on request.

Option A would lead to time pressure to reassess the criticality or importance of third-party arrangements and update the register for non-ICT TPAs, and this option might therefore increase the implementation costs. In addition, it might not be possible to renegotiate in parallel 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 be the same as Option B1 but introduces a different timeline for third-party arrangements that are not critical or important and leaves some supervisory flexibility regarding critical or important arrangements, where needed. Under Options B1 and B2 the period should be sufficient, as such a register might already exist at least for outsourcing arrangements and for DORA. Supervisory dialogue would be introduced regarding the 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 monitoring the transition, it would reduce the costs for financial entities, as the time pressure for renegotiation of contracts or, in some cases, the exit from third-party arrangements 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, identification of critical or important functions provided by third-party service providers and application of proportionality

Option A: relying on the definition provided in the Basel framework and the FSB toolkit, specifying that outsourcing arrangements are a subset of those TPAs, and setting stricter requirements for critical or important functions in accordance with DORA.

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

Using a common definition of third-party arrangements (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 and allow for a more proportionate approach. 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, including 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 required, taking into account the principle of proportionality and a risk-based approach that financial entities should implement to determine on which third-party arrangements they should focus, in line with their risk management framework. This would lead to only a minor additional administrative burden, as financial entities would already need to have in place some processes to manage their relevant risks, including those resulting from arrangements with TPSPs. In addition, a list of non-ICT services has also been excluded from the scope of application of the guidelines. In any case, financial entities must apply sound risk management processes, taking into account a risk-based approach, and would need to document their risk assessments. Having guidelines in place that specify the regulatory minimum expectations for such third-party arrangements that may still have some risks would provide a higher level of legal certainty. Costs for adjustments of internal processes should be minor as the framework is already in place for ICT third-party arrangements in accordance with DORA and existed under the previous EBA outsourcing guidelines.

Option B has been retained.

4) 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 or 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 the register of information). While the documentation regarding third-party arrangements needs to be extended beyond outsourcing arrangements, ICT third-party arrangements must be documented under the DORA framework. Several options have been considered.

Option A: requiring financial entities to document all third-party arrangements without specifying further the provision.

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 only to third-party arrangements supporting critical or 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 provisions for critical or important functions.

Option C: the same as Option B but requiring that planned third-party arrangements be documented in the register as soon as their implementation is likely.

Option D: the same as Option B, with the possibility that the non-ICT register under these Guidelines and the ICT register under DORA may be merged at the financial entity's discretion.

Option A would not result in a harmonised register across the EU that would be readily available for submission to the competent authority. Option A has therefore not been retained.

Option B would ensure that financial entities and competent authorities have an overview of all non-ICT-services-related third-party arrangements and are able to assess risk concentrations. By defining a minimum set of data points 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. Consistency with the DORA register needs 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 third-party arrangements would need to be included in the register. However, documentation would be necessary in any case, and such option would not be consistent with the DORA register, which captures all ICT third-party arrangements. By including a limited set of information (Option B2) for all third-party arrangements, the implementation of the register for non-ICT services would be more proportionate than Option B and consistent with the 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 into potential arrangements that would not come into effect, leading to minor additional costs for adding such arrangements to the register and potentially removing them afterwards. Furthermore, 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, consistent with DORA. The choice to merge the two registers would still belong to the financial entities.

Options B2 and D have been retained.

5) Guidelines on the assessment of risks and the criticality or importance of functions supported by third-party service providers and their ongoing 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 arrangements.

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 a harmonised framework but would further specify additional criteria for the assessment. A harmonised set of criteria to be implemented by financial entities would not create higher costs but would most likely trigger a tick the box approach. However, some of the criteria were already applicable under the outsourcing framework and are still relevant.

Option C would ensure that the criticality or importance of third-party arrangements would be determined by financial entities themselves in line with the definition provided under the guidelines. Under Option C, the Guidelines would provide a more specific framework for monitoring third-party risk. Additional costs would be limited to adjustments to the already existing risk management framework.

Options C have been retained.

6) 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 (EU) 2019/2034 (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, and competent authorities should therefore be informed before the implementation of third-party arrangements by financial entities.

Option B: the Guidelines should specify high-level principles regarding the supervision of third-party risk management by competent authorities leaving flexibility on the way they are informed regarding third-party arrangements.

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 would imply ex-ante notification and could therefore lead to some delays due to very burdensome

processes. 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 regarding third-party risk management.

Option B has been retained.

E. Cost-benefit analysis

The Guidelines further specify a limited set of specific provisions for financial entities and competent authorities compared with the previous outsourcing framework by providing clarification and consistency with DORA.

A higher level of clarity on third-party risk management benefits financial entities by creating a higher level of harmonisation regarding regulatory requirements and supervisory convergence. Standardised requirements lead to a reduction in costs for implementing processes, in particular when assessed on a consolidated basis.

The identification and supervision of third-party risks by competent authorities have a positive effect on the stability of the EU financial system. However, this means that competent authorities will have to assign more resources to the supervision of such risks. Those costs should be limited, as most of the provisions are limited to third-party arrangements supporting critical or important functions, consistently with DORA, and both financial entities and competent authorities are already familiar with the framework.

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

a. For initial addressees (i.e. 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 under the previous EBA Guidelines on outsourcing. Therefore, the additional costs triggered by the Guidelines should be limited overall.

b. For new addressees (i.e. Class 1 minus investment firms, Class 2 investment firms, and ARTs issuers) considering that the sectoral directives already establish a set of requirements for outsourcing that is quite detailed, the additional costs should be limited. In any case, all addressees are also already subject to DORA requirements.

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)	Very limited additional costs, because they already had to implement the previous Guidelines on outsourcing	Reduction in costs for implementing processes due to standardised requirements Reduction of ongoing costs for negotiating third-party arrangements with service providers due to a non-negotiable set of contractual conditions to be agreed on. Level playing field across all entity types and consistency with DORA Proportionality, due to the focus on critical or important outsourcing
Payment institutions and e-money institutions (already within scope)	Very limited additional costs, because they 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	Limited additional costs, because they already had to implement the previous Guidelines on outsourcing, but also need to ensure compliance with these guidelines and DORA	
Class 1 minus investment firms and Class 2 investment firms	Limited additional costs (due to IFD internal governance requirements, MIFID, and DORA)	
ART issuers	Limited additional costs (due to MICAR internal governance requirements and DORA)	
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	
Competent authorities	Higher supervision costs due to increased scope of application of guidelines	Increased efficiency of supervision, due to increased

		harmonisation, and proportionality Ensured harmonised practices and supervisory convergence Stability of the EU financial system

4.2 Feedback on the public consultation and on the opinion of the BSG

The EBA publicly consulted on the draft proposal contained in this paper. The consultation period lasted for three months and ended on 8 October 2025. Seventy-two (72) responses were received, and only non-confidential ones were published on the EBA website.

The draft Guidelines were also presented to the Banking Stakeholder Group (BSG) of the EBA.

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. This paper presents a summary of the key points and other comments arising from the public consultation, the analysis and discussion triggered by these comments, and the measures taken to address them if deemed necessary. The following table provides a summary of the responses to the consultation and the EBA's analysis.

2. Overall, the Guidelines have been reviewed to provide more proportionality, and more clarity regarding the scope, the focus on critical or important functions, and the alignment with the DORA framework. Furthermore, the transitional period has been adjusted for more flexibility regarding the update of the services provided by TPSPs supporting non-critical functions.

3. Regarding the register for non-ICT services, the Guidelines provide for sufficient flexibility and allow financial entities to combine it with the register under DORA or to keep a more proportionate one, as per the Guidelines, while maintaining consistency between the two.

4. In many cases, stakeholders made similar comments in response to different questions.

5. Changes have been incorporated into the Guidelines as a result of the responses received during the public consultation.

The BSG's opinion regarding the updated Guidelines submitted to public consultation

6. The BSG submitted an official response to the relevant consultation paper with key concerns:

— Alignment of definitions with DORA, especially regarding critical or important functions;

— Enhancement of proportionality by:

(a) focusing on contractual arrangements with TPSPs that involve significant risks to financial entities and on financial entities that have a material impact on the market,

(b) having a much more risk-based approach in line with the risk profile, the nature, and the business model of the financial entities and the complexity of their activities, with a

special focus on financial entities which are already regulated or supervised under EU laws (e.g. Class 2 investment firms, UCITS management companies and AIFMs that are subsidiaries of banking or investment-firm groups), and intragroup TPSPs; and

(c) extending proportionality as stated in Section 1 of Title I to other relevant titles and sections.

— Impact on the contractual relationships between credit institutions and TPSPs as to the requirements for termination rights, which may constitute an undue interference in the principle of contractual freedom.

— Cooperation with other CAs in the context of the management of third-party risks.

— Misalignment between the EBA impact analysis and the industry feedback on the costs of new regulations (Levels 2 and 3).

— The EBA's insight on the ongoing work on simplification and how this has been embedded in these Guidelines; and

— EBA–ESMA cooperation on this work regarding third-party risk, especially since ESMA has published 'Principles on third-party risk' (12 June 2025) with a different supervisory approach, even though it is addressed only to competent authorities only (NCAs).

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			
EBA legal mandate	Several respondents are questioning the EBA legal mandate for the extension of scope of the Guidelines (GLs) to all third-party agreements (beyond outsourcing agreements) while no legal provisions under CRD, IFD and MiFID II empowered the EBA to develop a comprehensive DORA-style regime covering all non-ICT related services provided by TPSPs to financial entities in the EU. In light of this, a few stakeholders advocate for the withdrawal of the GL, since the EBA could, after prior consultation with the industry, make use of non-binding Q&A to address specific issues for the management of third-party risks under CRD, MIFID 2 or IFD.	Directive 2013/36/EU (CRD) requires institutions to have sound governance arrangements and Article 74(3) CRD mandates the EBA to develop guidelines in this area. This includes the management of all risks including third-party risks. The same holds true for investment firms since Article 26 of Directive 2019/2034/EU (IFD) also sets out requirements for investment firms which are not considered to be small and non-interconnected to have robust governance arrangement and give the EBA, in consultation with ESMA, the mandate to issue guidelines in this area[64]. Issuers of asset-referenced tokens (ARTs) in accordance with Article 34 of Regulation (EU) 2023/1114 (MiCAR) should have robust internal governance arrangements. In this regard, 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 ARTs. Finally, payment institutions in line with Article 11 of Directive 2015/2366/EU (PSD2) should have sound governance arrangements. Third-party risk is one of the risks that financial entities should manage.	No change
Redundant regulation / Interactions between	Some respondents highlight that the provisions on conflicts of interest, business continuity plans, and the	The objective of the update of the Guidelines on outsourcing arrangements is to ensure alignment	No change

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

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
EBA GL and national laws	internal audit function are, in many cases, duplicative of existing regulations. This "double regulation" adds to regulatory fragmentation, which runs counter to the goal of achieving a single rulebook. Such fragmentation may undermine the effectiveness and resilience of the regulatory framework. Another respondent notes a disconnect between EBA Guidelines and expectations under national law. For the clear application of the Guidelines, it will be important to ensure clarity on which of the acts will the financial entity be expected to comply with.	between the management of third-party risk regarding non-ICT services and the DORA framework regarding ICT services. This update will ensure a consistent and coherent application by financial entities and ensure supervisory convergence across the EU. In line with Article 16 of Regulation (EU) No 1093/2010 (EBA founding regulation), the competent authorities and financial institutions have to make every effort to comply with those Guidelines. Within 2 months of the issuance of Guidelines each competent authority is required to confirm whether it complies or intends to comply with those Guidelines. In the event that a competent authority does not comply or does not intend to comply, it has to inform the EBA, stating its reasons.	
Overlaps between EBA draft GL and CSDR	Respondent advocates for stronger coordination between the Guidelines and the CSDR framework to eliminate unnecessary duplication and regulatory fragmentation. The definitions and obligations linked to outsourcing and Critical Service Providers (CSPs) under CSDR diverge from those under DORA and the draft Guidelines, despite targeting similar risk domains. This misalignment results in a proliferation of supplier classifications at group level — outsourcing, ICT, non-ICT, CIF, non-CIF, CSP, BRRD-critical— creating operational inefficiencies and compliance complexity.	The CSDR framework (Regulation (EU) No 909/2014) applies to central securities depositories (CSDs) to promote safe, efficient and smooth settlement where CSD refers to a legal person that operates a securities settlement system and provides at least one other core service listed in Section A of the Annex – i.e. notary service, central maintenance service and settlement service (Art. 2(1), point 1). In light of the above, the CSD firms are not within the scope of these GLs.	No change
Extension of scope – Proportionality	Most of the respondents argue for a more proportionate and risk-based approach in light of the updated scope of the Guidelines, highlighting concerns that some provisions could create unnecessary administrative burdens.	The 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	The GLs have been amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	In this context, some respondents suggest that proportionality should be more thoroughly integrated into the GL's requirements for contractual clauses, due diligence, intragroup arrangements and the register, and that specific criteria should be introduced to allow financial entities to qualify third-party arrangements (TPAs) which have a real impact on their operational resilience and business continuity.	and complexity of its activities. The Guidelines further specify the application of proportionality by providing a non-exhaustive list of criteria to consider when applying the Guidelines. In addition, the Guidelines put a clear focus on critical or important functions supported by TPSP. Some specific guidelines on the register for non-ICT services have been provided considering a proportionate approach to reduce the burden for both financial entities and competent authorities. The same holds true for the section on policy and the guidelines in general.	
Lack of Clarity on Third-Party Services in Scope	Some respondents highlight a lack of clear distinctions between third-party services in scope under the Guidelines as compared to the DORA Regulation. For example, under DORA, regulated services such as global network structures, legally required functions, and global financial messaging infrastructures are exempted, whereas the proposed Guidelines lack clarity on whether services subject to regulatory or licensing regimes (e.g., credit institutions) are included or exempted.	The Guidelines exclude from their scope of application specific regulated activities under para. 32 (such as global network infrastructures, clearing and settlement arrangements, global financial messaging infrastructures), consistently with DORA. Additional exclusions have been added. The Guidelines have been further clarified regarding regulated services. Regulated financial services that are legally required to be performed by another financial entity regulated under Union law including by financial entities not in the scope of these guidelines but regulated under financial services Union law are excluded. It should be clarified that these entities may still act as a third-party services provider nevertheless when providing other types of services to another financial entity.	The Guidelines have been clarified
Interaction with GL IG	Some respondents suggest clarifying how far the Guidelines provisions may be interpreted in line with the structures and responsibilities under national company law and the EBA Guidelines on internal governance. In that	The Guidelines are intended to apply to all existing board structures without interfering with the general allocation of competences in accordance with national company law or advocating any particular structure.	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	sense, when the Guidelines refer to the various concepts of "management function", "senior management" and "key function holder", those terms are not properly defined.	Accordingly, they should be applied irrespective of the board structure used (a unitary and/or a dual board structure and/or another structure) across Member States. The terms 'management body in its management function' and 'management body in its supervisory function' are used throughout these Guidelines without referring to any specific governance structure, and references to the management (executive) or supervisory (non-executive) function should be understood as applying to the bodies or members of the management body responsible for that function in accordance with national law. The various notions used (management body/ senior management and key function holders) are defined in Directive 2013/36/EU and in the respective sectoral legislation.	
Responses to questions in Consultation Paper EBA/CP/2025/12			
Question 1. Are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?			
Subject matter (para. 5-7)			
Regulated and/or supervised TPSP	Several respondents ask for the GL to further specify if regulated or supervised TPSP are also within the Guidelines' scope, since these companies are important for the financial entity's internal processes chain as they might provide services to them that those financial entities cannot or are not allowed to provide due to their license. Several respondents propose to exclude from the Guidelines services provided by regulated financial entities	When financial entities rely on supervised TPSP, this needs to be taken into account for the application of the proportionality principle and in the risk assessment; however, the provisions related to the management of third-party risk still apply. The Guidelines have been further clarified regarding regulated services. Regulated financial services that are legally required to be performed by another financial entity regulated under Union law including by financial entities not in the scope of these guidelines but regulated under	No change The Guidelines have been amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	in line with DORA as clarified in a recent Q&A (Q74 ESA Q&A).	financial services Union law are excluded. It should be clarified that these entities may still act as a third-party services provider nevertheless when providing other types of services to another financial entity.	
Intragroup TPSP	Some respondents consider that the GL do not sufficiently reflect the lower risk profile of intragroup outsourcing compared to external TPSPs. This unbalanced approach may discourage the use of efficient and well-controlled intragroup models. In that sense, some respondents ask to clarify how far an intragroup TPSP can be seen as a third-party within the Guidelines, since an intra-group TPSP does not require an arrangement.	The Guidelines recognise the difference between intragroup arrangements and arrangements with TPSPs outside of the group. Intragroup arrangements (including within IPS) can indeed be cost effective and efficient ways of receiving or sharing services however they may still have risks. Therefore, the same provisions apply to both situations. Some flexibility has been already introduced when relying on intragroup service providers.	No change
ICT/non-ICT services	Some respondents ask for providing a clear and consistent definition of what constitutes ICT services to ensure full coherence between DORA and those GL. Several respondents note that the scoping decision regarding application of DORA or the Guidelines (including hybrid ICT and non-ICT services) is very complex and includes a materiality determination. The Guidelines should further clarify and supplement the objective criteria and thresholds that should be used in making this determination. Also, examples and facilitation of early engagement of supervisors should be added. In light of this, the same respondents ask for clarifying the classification of “hybrid services” provided by TPSP (i.e. services integrating ICT components but not related only to ICT or where the primary service is non-ICT but relies on ICT components in the delivery chain).	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 (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. It belongs to financial entities to determine what falls under ICT services and non-ICT services. The objective of the guidelines is to bridge the gap between the two and to ensure that financial entities have a holistic approach regarding their third-party risk management. ESAs Q&A DORA030 clarifies the definition of ICT services, while ESAs Q&A DORA095 clarifies the applicable framework when the third-party	

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		arrangement between a financial institution and a direct TPSP relates to non-ICT services but ICT services to support critical or important functions are provided by subcontractors. Additionally, ESAs Q&A DORA095 clarifies the identification of ICT TPSP regarding the type of service provided. Those two Q&A- have been taken into account by the Guidelines.	
Scope of application (para. 12-14)			
Class 2 and Class 3 IF	Some respondents point out that the scope of the GL is too broad regarding investment firms, considering that the EBA is exceeding the legal mandate while Class 2 investment firms are generally not systemically relevant and are already subject to comprehensive governance and risk management requirements under the IFD/IFR framework.	In line with the prudential framework for investment firms under Directive 2019/2034/EU (IFD), Class 2 investment firms are required to have sound governance arrangements (Article 26 of IFD) and should therefore be covered by the GLs. 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 these Guidelines. However, they are still subject to the MiFID framework. ESMA is involved in the development of these Guidelines and their principles on third-party risks supervision have been taken into account. It should also be mentioned that all IF are covered by DORA.	No change
UCITS and AIFMs	Some respondents note that UCITS management companies and AIFMs that are subsidiaries of banking or investment-firm groups would fall indirectly within the GL's scope, considering this exceeds the EBA legal mandate and would create significant legal uncertainty and overlaps with the existing ESMA framework (ESMA Principles on third-party risks supervision), especially in group contexts	In accordance with Article 109(2) of Directive 2013/36/EU, these Guidelines apply on a consolidated and sub-consolidated basis taking into account the prudential scope of consolidation. UCITS and AIFMD firms, as financial institutions, are part of the prudential scope of consolidation. In this regard, the EU parent undertaking or the parent undertaking of a banking	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	where functions are delegated across entities or regarding depositary relationships under AIFMD and UCITS which are already regulated functions. Few respondents suggest that the European Union should allow regulated firms to opt-in to a standardised EBA register which is consistent with the DORA register. This would enable domestic firms to comply in the manner most appropriate to their arrangements and would enable firms operating across Member States to unify their operations and reporting requirements.	group in a Member State should ensure that internal governance arrangements, processes and mechanisms in their subsidiaries are consistent, well integrated and adequate for the effective application of these Guidelines. The same holds true for investment group in accordance with Directive 2019/2034/EU (IFD). However, this is without prejudice of the UCITS and AIFMD framework regarding delegation; in particular, the application of such sectoral rules by UCITS and AIFMD firms can also ensure compliance with these Guidelines on a consolidated and/or sub-consolidated basis. Regarding depositary services provided to AIFMD and UCITS firms, they are excluded from the application of these Guidelines even on a consolidated and/or sub-consolidated basis, since these are regulated services provided by regulated financial entities. The register is consistent with the DORA register and financial entities have the possibility to combine it with the DORA register under Article 28(3) DORA.	No change
Institutional Protection Scheme (IPS)	A few respondents indicate that the wording "TPSPs within the group or the institutional protection scheme" does not adequately capture the variety of financial entities which could fall under this qualification. A clearer alternative is suggested: "TPSPs within group- or institutional protection scheme (IPS)-related structures".	The wording used is fully correct and consistent with Directive 2013/36/EU and Regulation (EU) 575/2013.	No change
Group approach	Some respondents ask for an explicit statement that the groupwide consolidated approach is limited only to those financial entities of that group that are also identified as addressees within the scope of the GL. In this regard, they	In accordance with Article 109(2) of Directive 2013/36/EU, these Guidelines apply on a consolidated and sub-consolidated basis taking into account the prudential scope of consolidation. UCITS management companies and AIFM are financial institutions and as	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	ask for a more proportionate approach, reducing the regulatory burden for intra-group TPSPs.	such are part of the prudential scope of consolidation. In this regard, the EU parent undertaking or the parent undertaking in a Member State should ensure that internal governance arrangements, processes and mechanisms in their subsidiaries are consistent, well integrated and adequate for the effective application of these Guidelines. The same holds true for investment group in accordance with Directive 2019/2034/EU (IFD). However, this is without prejudice of UCITS and AIFMD framework regarding the application of requirements on delegation.	
Agreement between branches	A few respondents are wondering if agreements between branches of an EU credit institution and/or between the parent company and an EU branch of an EU credit institution should be considered as out of the scope of the Guidelines.	An EU branch of an EU credit institution does not have legal personality; as such an EU branch of an EU credit institution is the same legal entity and therefore an agreement is not possible; however, an EU branch of an EU credit institution relying on non-ICT services supported by another entity within the group are within the scope of these Guidelines (intragroup arrangements). EU branches of third country credit institutions (third country branches) within the meaning of Article 47 of Directive 2013/36/EU, do not have the legal personality and are not considered as separate legal entities from their head undertaking in the third country. Therefore, a proportionate approach is appropriate for the application of these guidelines. In this regard, while a written contract between the head undertaking and its EU branch is not possible as they are not legally distinct, the EU branch should have any other arrangement (such as Service Level arrangement or policies) which comply with these guidelines.	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Third-country TPSP	Some respondents seek clarification on the treatment of third-country TPSPs contracted through intragroup entities.	When a financial entity relies on an intragroup TPSP located in a third country, the EU financial entity should comply with the Guidelines and consider in its risk assessment that the TPSP is located in a third country.	No change
MiCAR – ART issuers and CASP	While most of the respondents acknowledge the fact that ART issuers are within the Guidelines (if not already covered as CI), some respondents raise that the exclusion of crypto-asset service providers represents an unjustified difference in treatment compared to financial entities already included in the Guidelines and which are providing crypto-assets services.	CASP are not within the remit of EBAs scope of action and are not addressees of these Guidelines and therefore not in scope of these Guidelines. It should be noted however that Article 73 of MICAR regulates outsourcing for crypto-asset service providers.	No change
Definitions (para. 16)			
Distinction between TPA and outsourcing	Most of the respondents note that the definition of "outsourcing" is not fully aligned with DORA in relation to the time criterion – ie. DORA refers only to "an ongoing basis" whereas the GL to "a recurrent or an ongoing basis". A few respondents suggest limiting the definition of a third-party agreement (TPA) to services performed "on a recurrent or ongoing basis" for a more proportionate approach. Moreover, some respondents criticise that the key difference between a TPA and an outsourcing agreement is unclear. In that sense, those respondents require for some clarification on whether financial entities will still be required to identify, track and/or tag their outsourcing arrangements - including those supporting critical and important functions - amongst their population of TPAs for any purpose under the Guidelines.	The "outsourcing" definition is in line with the definition of outsourcing under the 2019 EBA Guidelines on outsourcing arrangements and the FSB toolkit "Enhancing Third-Party Risk Management and Oversight" published in December 2023. DORA does not include a definition of outsourcing, and the definition of third-party arrangements is in line with BCBS principles. The draft has been adapted to include "on an ongoing basis" or "recurrent basis". Outsourcing is a subset of third-party arrangements and within the scope of the guidelines.	The Guidelines have been amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
TPA – supporting critical or important functions	Some respondents suggest having in the Guidelines only material third-party arrangements that support a critical or important function.	To be consistent with the DORA framework, the Guidelines cover all third-party arrangements. However, the focus is on third party arrangements supporting a critical or important function with more stringent provisions applicable to them. However, other arrangements should also be managed by financial entities on a risk-based approach as part of their governance arrangements. The Guidelines have been clarified to better reflect this distinction and the respective applicable provisions	The guidelines have been clarified
Distinction between functions and services	Some respondents raised their concerns about the inconsistent and/or interchangeable use of wordings "*function*", "*service*", "*arrangement*", and "*activity*" throughout the Guidelines, which creates confusion and complexity, and does not align with the approach taken under DORA. In that sense, they note that the term "function" is used in the GL as a synonym to "service".	The Guidelines have been clarified to be consistent with the wording under with DORA.	The Guidelines have been clarified
Function / subfunction – classification as CIF	A few respondents note that some functions have sub-functions whose disruption could impact a financial entity's soundness or compliance, while others would not. The respondent suggests clearer guidance on whether sub-functions should fall within the GL's scope.	The Guidelines have been clarified to focus on arrangements supporting critical or important functions. Consequently, a part of a function, whose disruption could impact a financial entity's soundness, financial performance or compliance would fall within the scope of the Guidelines. The Guidelines now also refer to "non-ICT services supporting critical or important functions provided by TPSP" and only the subcontractors that effectively underpin the provision of services supporting critical or important functions should be captured in the scope of monitoring and the register.	The Guidelines have been clarified

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Subcontracting	Some respondents suggest aligning the terminology and/or the concept with DORA to support a consistent approach across the two frameworks and to properly reflect a risk-based approach for the supply-chain.	See comments above	The Guidelines have been clarified
Critical or important functions – DORA alignment	Several respondents point out the fact that while the definition of "critical or important function" in the GL is aligned with DORA, the use of the term is not consistent with the approach under DORA. While an arrangement with a TPSP may "support" a critical or important function of the financial entity under DORA, it does not establish such a function.	The wording in the Guidelines has been clarified to accommodate the comment.	The Guidelines have been amended
Critical or important functions – BRRD alignment	A few respondents seek for a closer alignment of the definition of a "critical or important function" with the BRRD framework. While the Guidelines indicate that the definition also includes "critical functions" as defined in Article 2(1), point (35) of the BRRD.	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.	No change
Critical or important functions – identification, alignment with DORA	Several respondents consider that the approach to determine "critical or important functions" between DORA and the Guidelines is not aligned, especially in relation to the risk management for the provision of both ICT and non-ICT services.	The Guidelines are consistent with the DORA framework regarding the approach to determine a critical or important function. A definition of "critical or important function" has been provided. It belongs to the financial entities to perform this assessment.	The guidelines have been clarified
Critical or important functions – Pre-	Some respondents identify that the Guidelines specify that financial entities "should inform competent authorities in a timely manner and, where appropriate, engage in a supervisory dialogue with the competent authorities about	This further specification may be done by CAs for the purpose of supervision.	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
notification to competent authorities	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", but no timeframe is specified.		
Concentration risk	A few respondents point out that the definition of concentration risk might be ambiguous, especially when referring to "other types of adverse effects". Thus, they suggest either specifying a positive list of defined risks to be included or clarifying that only significant and severe adverse impacts should fall within the definition.	The definition is consistent with the DORA framework, and it belongs to the financial entities to determine what types of adverse effects they may be exposed to. This includes the risk of large losses.	No change
Date of application and Transitional arrangements (para. 17-20)			
2-year period – extension of the transitional period	Some respondents ask for a delay in the date of application to allow the incorporation of the provisions of the Guidelines in any contract due for renewal. They suggest introducing a window between the publication and the entry into force of the GL from 9-month to 18-month. In addition, most of the respondents support the 2-year transitional period. Some others ask for an additional fixed transitional period applying to third-party arrangements of critical or important functions and for introducing a "best-effort" clause with regard to the remaining non-ICT services.	The 2-year transitional period is considered an adequate timeline. Thus, where the review of third-party arrangements of critical or important functions and the documentation of all existing third-party arrangement are not finalised within 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 and the documentation. More flexibility has been introduced for the update of arrangements supporting non-critical or non-important functions.	The Guidelines have been amended
Implementation – set of contractual clauses	A few respondents advocate for a minimum set of contractual clauses subject to regulatory enforcement and aligned with the DORA framework to allow for easier	The Guidelines specify the set of contractual clauses that should be in a written agreement between financial entities and TPSP. This is consistent with the DORA framework and international standards. It belongs to financial entities to insert and implement	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	review and implementation of the contractual conditions by the financial entities.	these clauses into their contracts with third parties particularly when they related to critical or important functions.	
Question 2. Is Title II appropriate and sufficiently clear?			
Sound management of TPR (para. 30-32)			
Recurrent or Ongoing Basis Specification of Duration (para. 30)	Several respondents note that the outsourcing definition includes "recurrent or ongoing basis", while the third-party arrangement definition does not. The respondents request clarification whether the Guidelines intend to apply this criterium for outsourcing and for third-party arrangements.	The "outsourcing" definition is in line with the existing definition of outsourcing under the 2019 EBA Guidelines on outsourcing arrangements and the FSB toolkit "Enhancing Third-Party Risk Management and Oversight" published in December 2023. The definition of third-party arrangements is aligned with DORA, and the draft has been adapted to include "on an ongoing basis or recurrent basis".	The Guidelines have been amended
Taxonomy of out-of-scope functions (para. 32)	Several respondents point out that the list of functions excluded from the Guidelines scope under para. 32 is too narrow and might conflict with the definition of TPA under para. 16. In this regard, they consider that the GL would not only cover material non-ICT services but also extend to other services provided by TPSPs which regularly do not have a material impact on financial entities' risk exposures or their operational resilience.	The Guidelines specify further a list of functions/activities excluded from the scope of application of the Guidelines (see para. 32). The paragraph has been amended and clarified.	The Guidelines have been amended
Exclusion - Market Information Services (para. 32)	Several respondents suggest adding an exclusion for market information services (e.g. Bloomberg, Moody's, Standard & Poor's, Fitch) as they exclusively fall under DORA in order to avoid misunderstandings.	The Guidelines have been amended to accommodate the comment and exclude market information services under para. 32 of the Guidelines in line with the FSB toolkit.	The Guidelines have been amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Exclusion – other requests (para. 32)	Some respondents proposed that functions that may be delegated by asset managers under Article 20 of the AIFMD and Article 13 of the UCITS Directive be excluded. Additionally, CSDs as well as by custodians and settlement agents should be added to c). Some respondents suggested to include local providers like payment scheme operators (not cards) alongside global network infrastructure such as Visa and Mastercard. Other respondents argue against the lack of specific exemptions for local providers of market data services and network infrastructure services in both draft and existing EBA outsourcing Guidelines. These omissions potentially create unfair advantages for larger international firms while imposing significant implementation costs on smaller, local companies.	UCITS and AIFMD firms are not addressees of the Guidelines. However, in accordance with Article 109(2) of Directive 2013/36/EU, these Guidelines apply on a consolidated and sub-consolidated basis taking into account the prudential scope of consolidation. This is without prejudice of UCITS and AIFMD framework regarding delegation; in particular, the application of such sectoral rules by UCITS and AIFMD firms can also ensure compliance with these Guidelines on a consolidated and/or sub-consolidated basis. The Guidelines (para. 32) have been clarified to accommodate the comments.	The Guidelines have been clarified
Exclusion – FSB toolkit (para. 32)	Several respondents ask for exclusions identical in scope with the FSB toolkit on third-party risk management.	The exclusions under para. 32 of the Guidelines are consistent with the FSB toolkit;	The Guidelines have been amended
Exclusion – material risk impact (para. 32 f)	Several respondents highlight concerns over the introduction of an exclusion criterion related to "material impact on risk exposure and operational resilience" due to potential inconsistencies in interpretation across different financial institutions and regulatory bodies. This approach could result in varying assessments and increased burdens on financial institutions regarding assessments and monitoring.	See comments above. The par. 32 has been amended and clarified.	The Guidelines have been clarified

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Exclusion – material risk impact – extension (para. 32 f)	Some respondents suggest extending the ability to exclude services due to immaterial risk impact to subcontractors in the service's supply chain. Other respondents proposed to add an extensive list of exempted services (e.g. printing services, construction/building services, marketing/brand related services, learning, sponsorship arrangements).	The Paragraph 32 of the Guidelines has been amended and clarified. The point regarding subcontractors has been accommodated to focus on the ones effectively underpinning a critical or important function.	The Guidelines have been amended
Critical or important functions (para. 33-37)			
CIF assessment (para. 33)	Some respondents seek clarification on interpreting risk assessments of third-party arrangements to classify functions as critical or important. Those respondents request details on key evaluation criteria and operational approaches for assessing risks such as operational, reputational, legal, and concentration risks.	The Guidelines already provide for a definition of the notion of critical or important function. It belongs to the financial entity to determine which functions are critical or important.	The guidelines have been clarified
CIF - compliance with Financial Services Law (para. 33 a)	Several respondents note that "*where the failure of the function would materially impair the continuing compliance of a financial entity with its obligations under applicable financial services law"* is vague and could be understood to encompass many or most activities in a financial institution as there is a wide range of relevant laws, while not impacting operational resilience or risk.	This is fully in line with the definition of "critical or important function" under DORA. It belongs to the financial entity to determine which function is critical or important in line with the definition and their own risk assessment.	No change
CIF – internal control (para. 34)	Some respondents request a clarifying definition of internal control and whether, in case an internal control function is performed by a third-party, it would automatically qualify as an CIF. Other respondents add that there should be a de minimis threshold for such cases.	Internal control functions are those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance. This includes the compliance function, the risk management function including control function to manage and oversee ICT risk as referred to in article 6(4) of Regulation (EU) 2022/2554, and the internal audit function. The Guidelines are already clear and	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		specify that, 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.	
Adverse impact – wording (para. 36)	Some respondents propose to add "material" to "adverse impact".	The Guidelines have been clarified.	The Guidelines have been amended
CIF classification – factors – clarification (para. 37)	Some respondents seek clarity on whether the factors mentioned under para. 37, points (a) and (b) need to be evaluated jointly ("AND") or separately ("OR"). Guidance on interpreting the term "at least" to avoid differing understandings among financial institutions regarding what constitutes a critical function is requested.	The Guidelines have been amended. It belongs to the financial entity to determine which function is critical or important in line with the definition and their own risk assessment.	The guidelines have been amended
Authentication / Authorisation of payment	A few respondents ask for clarification that "authentication and authorisation" are not deemed critical or important functions, as a failure would not significantly impact service provision or control functions Additionally, when the issuer maintains direct oversight of authentication and authorization, particularly leveraging off-the-shelf technologies like biometric readers integrated into consumer devices, it avoids qualifying these actions as Strong Customer Authentication (SCA) delegation or outsourcing according to the European Banking Authority (EBA)'s stance outlined in the PSD2 review of June 2022.	Authentication, including strong customer authentication (SCA), as defined in the Payment Services Directive can be deemed as a "critical or important function" according to the definition in these Guidelines. EBA is actually mandated to develop RTS on SCA and outsourcing under PSD3.	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Question 3. Are Sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?			
Section 5 – Sound governance arrangements and third-party risk (para. 38 – 47)			
Content of the strategy on the sound management of third-party risks (para. 38)	Some respondents seek clarity and/or guidance as to what should be included in the strategy on the sound management of third-party risk which is defined, approved and regularly reviewed by the MB.	It belongs to financial entities to define their own strategy adapted to their business needs and according to their risk appetite.	No change
Policy, external suppliers, and responsibilities	Some respondents are wondering how far the ownership of the policy for managing external suppliers in the FE's structure should be assigned to one single unit or more.	It belongs to financial entities to develop their own third-party risk management policy in accordance with the Guidelines and involved internally the various functions where necessary or appropriate.	No change
Strategy and Policy on Third-Party Risk (para. 38)	Some respondents ask for more clarity on the distinction between the strategy and the policy on the sound management of third-party risks – which imply different responsibilities. In that sense, they ask for clearer definitions of the components of the overarching third-party risk strategy. Besides, they suggest clarifying that a regular assessment of risks by the financial institution itself – rather than by the management body – should be sufficient and allowing flexibility to develop either integrated or separate strategies for non-ICT and ICT services.	Consistently with DORA, the strategy on third-party risk should include a policy on the use of services supporting critical or important functions provided by TPSPs. The guidelines have been amended to be consistent with DORA. Financial entities have the flexibility to develop either integrated or separate strategies regarding third-party risk management (for non-ICT and ICT services).	The Guidelines have been clarified
Risk assessment and proportionality (para. 40)	Some respondents suggest clarifying that arrangements not covered under Section 3 are not included in the financial entity's operational risk management on a general basis since detailed individual risk assessments in accordance with Section 11.2 – also for arrangements or	The paragraph and Section 5 have been clarified.	The Guidelines have been clarified

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	services that are not even covered by the GLs – would be disproportionate.		
Remove para. 41 as redundant	Some respondents consider that para. 41 of the GLs is redundant as the GDPR already applies to financial institutions. This point is reiterated under para. 47(g) of the Guidelines.	The comment has been accommodated.	The Guidelines have been amended
Reference to 'payments institutions' unclear (para. 44)	Some respondents consider that according to the Guidelines, "financial entities" already include payment institutions, there is no need to explicitly distinguish them again within this provision.	In this case, the reference to payment institution is made in accordance with Articles 5(1), point (n) Directive (EU) 2015/2366 as specific requirement applies.	The Guidelines have been clarified
Duplication with CRD and EBA Guidelines on Internal Governance (para. 43 and 45, points (a) and (b))	Some respondents outline that the provisions under paragraph 43 are already addressed under CRD which may lead to unnecessary uncertainty. They stress that it is unrealistic for the management body of a financial institution to oversee all potential conflicts of interest at TPSPs.	Para. 43 of the Guidelines should be kept since some financial entities within the scope of these Guidelines are not within the scope of the EBA Guidelines on Internal Governance. The wording related to the responsibility of the management body with regard to conflict of interest has been amended to accommodate the comment.	The Guidelines have been clarified
Assign responsibility to a specific member (para. 45, points (a) and (c))	Respondent proposes that the responsibilities be assigned to the specific member of the management body responsible for the relevant function, rather than to the management body as a whole.	The management body is a collegial body and as such is responsible collectively.	No change
	Similarly, another respondent claims it is unclear if the responsibilities are the same for a person with an "established role" as for a "designated member of senior management". The "established role" should monitor TP arrangements, whereas the "member of senior	Financial entities can either designate a specific role dedicated to the monitoring of third-party arrangements or designate a member of senior management as directly accountable to the management body responsible for overseeing third-party arrangements (for example, the risk management function or the compliance function). The	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	management", if designated, seems to have further reaching responsibilities.	responsibilities assigned are the same for both. Less complex financial entities may assign the role to a member of the financial entity's management body.	
Provisions for using TPSP for CIFs (para. 47 (f))	Some respondents indicate that the provision under Paragraph 47(f) is vague and may be unrealistic depending on how "appropriate timeframe" is interpreted. It also does not consider potential remedial measures for deficiencies at the TPSP. They recommend either deleting point (f) or replacing it with a more general reference to appropriate business continuity management and exit strategies.	Financial entities should have an exit strategy. An exit plan is required for each contractual arrangement supporting critical or important functions. There should be no confusion between business continuity plans and exit plans. Service disruptions need to be taken into account for exit planning when they are unforeseen and persistent. The appropriate timeframe is to be defined by financial entities according to the specific circumstances.	No change
Section 6 – Policy on third-party risk management (para. 48 – 54)			
Annual review not mandatory, alignment with CRD, and overlaps (para. 48)	Some respondents suggest that an annual review of the third-party risk management policy should not be mandatory. Instead, regular reviews and, where necessary, event-related reviews, would be sufficient. A respondent argues that it would be advisable to leave the institutions the choice of whether they want to combine the outsourcing policy (introduced according to the EBA Guidelines on outsourcing arrangements from 2019) with the third-party risk management policy and have one document or two separate ones.	The review of the policy on a yearly basis is reasonable and not burdensome in the case the policy has not changed. This is also consistent with DORA. Flexibility is given to financial entities as long as the policy complies with the provisions set out under these Guidelines.	The guidelines have been clarified

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
DORA Alignment - wording of designated role, ICT/non-ICT functions (para. 49-50)	Some respondents suggest that para. 49 of the Guidelines should be amended to align the wording with DORA requirements.	The paragraph 49 has been aligned consistently with DORA.	The Guidelines have been clarified
	Few respondents suggest that under point (d), a footnote akin to footnote 51 should be added: "This role and the reporting-line 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."	The comment has been accommodated.	The Guidelines have been amended
	Several respondents express disagreement with the need for policy-level differentiation between ICT and non-ICT functions as stated in para. 50. ICT and non-ICT functions at a financial entity are organically connected, and risks cascade across both, so policy language should not create any distinction between them, focusing instead on what are commonly shared risks. They recommend that the GL either encourage financial entities to adopt a unified third-party risk management policy that integrates both ICT risks and non-ICT risks or allows for more flexibility.	The comment has been accommodated. Financial institutions have the flexibility to develop either integrated or separate policies regarding third-party risk management (for non-ICT and ICT services).	The Guidelines have been clarified
Ultimate responsibility (para. 49 (b))	Some respondents ask for removing para. 49 (b) since the financial entities are responsible for ensuring compliance with all applicable legal and regulatory requirements when using third-party arrangements regardless of what is stated in a policy.	The comment has been accommodated.	The guidelines have been amended
Suggestions and clarifications on para. 49 (h)	While a respondent suggests that para. 49, point (h) should be replaced by a reference to Section 14, another respondent seeks clarification on that same para. regarding "where such an exit is considered possible".	The comment has been accommodated and the cross reference added. Financial entities should ensure that they are able to exit third-party arrangements without undue	The Guidelines have been clarified

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		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. It may not always be possible to exit an arrangement without any impact on the performance of the function; therefore business continuity measures should be implemented.	No change
Section 7 – Conflict of interests (para. 52 – 54)			
Conflict of interest - Definition (para. 53)	A few respondents seek for clarification on what exactly is meant by "material" conflicts of interest.	It belongs to financial entities to define the materiality threshold according to their own risk assessment.	No change
Delete para. 54	Several respondents recommend deleting Paragraph 54 from the Guidelines since a similar requirement was originally proposed in a delegated act under DORA but was not retained in the final text.	The paragraph has been amended to align with the Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024.	The Guidelines have been clarified
Section 8 – Business continuity plans (para. 55 – 58)			
Time-critical processes and BCPs (para. 55)	Some respondents suggest a reference to time-critical processes or functions, in addition to critical or important functions, to allow for a cumulative approach where both characteristics (criticality and time-criticality) are met.	The Guidelines are clear and consistent with existing standards including with DORA.	No change
BCP – scope of application (para. 55)	Some respondents suggest clarifying that not all CIFs may require a dedicated BCP, depending, for example, on the nature of the function and the associated risk exposure whereas there may be TPSPs which are not critical but support a CIF and assume no plan is needed in this instance.	The Guidelines only refer to business continuity plans with regard to critical or important functions provided by TPSPs presuming that these are the ones associated with high-risk exposure. It then belongs to financial entities to perform their assessment. If the support to a critical or important function is not material, then it	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		belongs to the financial entities to do the assessment and to demonstrate it where appropriate.	
Definition of "Unacceptable Level" (para. 56)	A few respondents suggest clarifying the term "unacceptable level" which does not align with existing definitions of business impact.	It belongs to financial entities to determine indicators and the thresholds in order to define what is an unacceptable level.	No change
Section 9 – Internal audit (para. 59 – 60)			
Scope of audits	Some respondents consider that many TPSPs currently assume that the right of competent authorities to examine or audit is always pre-scheduled, with some arrangements including a notice period of 14 days, which makes it impossible for authorities to carry out ad-hoc requests when needed. Hence, further clarification may be required.	This is part of the supervisory tasks and therefore it is recommended to liaise with competent authorities	No change
Overlap with GLs on Internal Governance	Some respondents note that para. 60 of those Guidelines and para. 224 of the draft revised Guidelines on internal governance might be redundant; thus, para. 60 could be omitted.	The Guidelines apply also to addressees that are not in the scope of addressees of the EBA Guidelines on internal governance (e.g. payment institutions and electronic money institutions).	No change
Section 10 – Documentation requirements (para. 61 – 69)			
Proportionality and alignment with the DORA Register of information	Some respondents claim that the Guidelines both lack of risk sensitivity (as they are not appropriate for all FE) and are too prescriptive; thus, they require for a more risk-based approach regarding the register. Respondents ask for more alignment with the DORA register under Article 28(3) of Regulation (EU) 2022/2554.	The Guidelines apply considering the proportionality principle as further specified and follow a risk-based approach (see Title I, Title II and Title IV). They focus on the use of TPSP supporting critical or important functions to which stricter provisions apply. Regarding the documentation (register), the Guidelines consider the existing register of information and the consistency with the DORA one. The amount of data points is lower	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		compared to the DORA register, while still being consistent regarding the common information to be included. The Guidelines provide for sufficient flexibility, and it belongs to financial entities whether to establish a separate register as specified by Guidelines or to use the same datapoints as for the DORA register. However, the Guidelines cannot go to such level of details as the Commission Implementing Regulation (EU) 2024/2956; the drafting has been aligned with DORA.	The Guidelines have been clarified
One single register	Several respondents agree that one register would bring benefits. They favor a single third-party register framework that captures both ICT and non-ICT arrangements which should be achieved through a single aligned register, with data field requirements adapted to reflect proportionality and risk-based principles.	The Guidelines provide for sufficient flexibility and allow financial entities to combine the register with the one under DORA.	The guidelines have been clarified
Two separate registers and clarification on discrepancies	Some respondents raise their concerns about the additional burden brought with the new regulation and advocate explicitly maintaining two separate registers as they currently are and cautioned that separating registers by ICT/non-ICT could complicate processes and risk inadequate monitoring of outsourcing-relevant agreements.	See comment above.	The guidelines have been clarified
Focus only on critical or important functions	Several respondents suggest limiting the scope to non-ICT TPSP which support CIFs. They suggest maintaining non-ICT non-CIF arrangements internally at entity level.	The focus of the Guidelines is in any case on the non-ICT services supporting critical or important functions. However, financial entities have to map all their dependencies. This is fully consistent with DORA. The same approach should be foreseen within the Guidelines. The guidelines have been in general	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		amended to have a more targeted focus on arrangements supporting critical or important function while still being consistent with DORA.	
Retention period of five years (para. 61)	Several respondents suggest deleting the five-year retention period as in DORA, given the lack of relevance to risk management.	The provision regarding the retention has been amended to align with DORA.	The Guidelines have been clarified
Possibility of a central register appreciated not useful (para. 62)	Respondent welcomes the possibility of maintaining a central register for institutions belonging to the same group or institutional protection scheme (cf. para. 62).	The Guidelines provide for this possibility under Section 2 on "Management of third-party risks by financial entities within groups and institutions that are members of an institutional protection scheme" and para. 62.	No change
Dates: end date, renewal date and notice period (para. 63 (b))	Several respondents argue that the provision to provide an end date and reason for the termination should not apply as services that have been terminated during the reporting period would not be captured in the register. Additionally, they note that alignment with the DORA Register might be improved – eg. DORA only requires a notice period for third parties supporting CIFs or asks for the next renewal date if the contract allows for extensions.	Para. 63 b) is aligned with Commission Implementing Regulation (EU) 2024/2956 and therefore should be kept as it is. The comment has been addressed.	No change The Guidelines have been clarified
Para. 63 (c) cannot apply to individual institutions	Considering that para. 63, point c) is only relevant in the case of centralised register in accordance with para. 62, they ask that clarification be provided, taking into account individual institutions, for whom this would not be possible.	The comment has been accommodated and a cross reference to para. 62 has been added.	The Guidelines have been clarified
Remove reference to subcontractors from para. 63 (d)	Some respondents suggest removing the reference to a *subcontractor* in para. 63, point (d) *since* the Guidelines'	Subcontractors effectively underpinning non-ICT services supporting critical or important functions should be in the register.	The guidelines have been clarified

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Register is intended to record details of TPSPs that have a direct relationship with in-scope entities.		
Reduce provisions on inclusion of LEI/EUID (para. 63 (g)	Several respondents raise concerns and propose to be less restrictive regarding the provision of the LEI/EUID of for direct providers and alternative providers since the financial entity might not be in the position to negotiate with a supplier to get a LEI or an EUID. Thus, they suggest considering only the company name or a more general identifier like the company register number.	The Guidelines have amended to accommodate the comment.	The Guidelines have been clarified
Clarification on 'data processing' (para. 63 (h))	Respondent seeks clarification on the interpretation on 'data processing'. They note that, per definition, it is digital and therefore should be considered as an ICT service which is out of scope of these Guidelines.	The comment has been accommodated and the reference deleted.	The Guidelines have been clarified
Cost fields inconsistency (paras. 63(k) and 64(h))	Many respondents found the cost disclosure requirements for critical arrangements and third-party providers expenses inconsistent and confusing, noting that para. 63(k) requires "total annual expense or estimated cost of each direct TPSP" while para. 64(h) requires "estimated annual budget cost for the past year."	The guidelines have been clarified consistently with DORA and the Commission Implementing Regulation (EU) 2024/2956.	The Guidelines have been clarified
Data collection for CIF under para. 64 (b) and (c)	A few respondents seek clarification on (i) the type of audit envisaged under para. 64(b) (internal, external, supervisory, or TPSP's own audits), and (ii) whether both the last and next audits are to be reported.	Internal audits performed should be reported and where it has been performed by the TPSP own audit then the last one should be reported.	No change
Substitutability/reintegration only for CIFs (par. 64d)	A few respondents argue that the provisions on substitutability and reintegration assessments for all TPSPs is disproportionate and not risk sensitive. These data fields should only be required following a risk-based approach,	This paragraph applies only to non-ICT services supporting critical or important function provided by TPSPs.	No change

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	and in any case only for material TPSPs providing CIFs or material parts thereof.		
Notification requirement inconsistent with DORA (para. 67)	Some respondents ask to remove the notification under para. 67 for planned contractual arrangement concerning critical or important functions, as there is no similar requirement under DORA.	The paragraph is consistent fully with Article 28 of DORA.	No change
Centralised submission of notifications (para. 67)	Some respondents argue that for groups or institutions belonging to an institutional protection scheme, centralised submission by a central unit should in any case be permitted.	The Guidelines apply on consolidated or sub-consolidated basis in accordance with Section 2; a centralised submission is possible.	The Guidelines have been clarified
Limit notifications to CIFs (para. 68)	Some respondents indicate that the provision under Paragraph 68 to inform competent authorities 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" should be limited to contracts that support critical or important functions.	The comment has been accommodated and the Guidelines clarified.	The Guidelines have been clarified
Question 4. Is Title IV of the Guidelines appropriate and sufficiently clear?			
Pre-contractual analysis – subcontracting (para. 70)	Some respondents suggest including subcontractors in the precontractual analysis.	The paragraph already refers to Section 11.2 which refers to the use of subcontracting.	No change
Risk assessment – scope (para. 73-74)	Several respondents ask for a proportionate approach, where low-risk or non-critical arrangements are subject to lighter assessments; or clarifying that assessments should be qualitative or context-based. Others suggest that the scope of risk assessment has been broadened beyond	The risk assessment is the starting point for a risk-based approach, and all relevant risks should be considered to allow financial entities to implement a risk-based approach and lower or increase the intensity of the monitoring according to the level of criticality or	The Guidelines have been clarified

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	operational risk alone, explicitly including reputational, legal, and concentration risks as distinct risk categories, or mentioning "all risks" resulting in an impractical / not risk-based approach.	importance. The criteria mentioned are to be considered and are not exhaustive. Financial entities should form their own assessment.	
Risk assessment – critical or important and other functions (para. 74-78)	Several respondents suggest that the risk assessment section should be limited to or differentiate between critical or important functions and other functions.	The risk assessment includes the consideration of whether a function is critical or important.	No change
Risk assessment – concentration risk (para. 76)	Some respondents ask for clarification and comment that concentration risk is often dealt with at group level and not applicable to individual entities, or that the subsidiary may rely on group-level assessments.	The Guidelines apply on a consolidated basis or sub-consolidated basis also. Consequently, within a group this assessment can be performed at group level and entities belonging to the group can rely on it.	No change
Risk assessment – delineation (para. 77)	Some respondents suggest limiting the provisions under para. 77 by the wording "Where a critical or important third-party arrangement includes the possibility" to avoid a possible interpretation that a non-critical TPSPs may subcontract a service of higher risk that its own.	The comment has been accommodated.	The Guidelines have been amended
Due diligence - delineation (para. 80)	Several respondents ask for clarifications on whether financial entities can assess factors relevant for the specific TPAs. Other respondents highlight that point d) (supervision by competent authorities) is not relevant for all TPSPs, the majority of which are not supervised by competent authorities and suggests the deletion of this point d).	The factors to be assessed are to be assessed for the specific potential TPA. Regarding point d), some TPSP may also be subject to supervision by a competent authority and still act as a third-party service provider, and this should also be taken into account in accordance with Title 1 of the Guidelines.	No change
Due diligence – critical or important functions (para. 81)	Several respondents require clarification that geographical dependencies are the same as location-related risks (including risks linked to jurisdiction), with a view to avoid	The comment has been accommodated and the Guidelines clarified.	The Guidelines have been amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	disproportionate granular requirements (political, economic, financial risks).		
Due diligence – supply chain (para. 83)	Several respondents ask to avoid wide prescriptive language on supply chain / ESG/ human rights or limit it to FEs that also fall within the scope of the Corporate sustainability due diligence directive (CSDDD).	Financial entities should carefully pay attention to human rights and take into account the impact of their TPA on all stakeholders; this includes taking into account their social and environmental responsibilities. Such aspects are relevant when TPSPs are located in third countries – and consistent with Guidelines on the management of environmental, social and governance (ESG) risk.	No change The Guidelines have been clarified
Contractual phase – proportionality (Section 12)	Several respondents think that contractual provisions of Section 12 are too detailed, with a level of granularity that imposes a significant burden on financial institutions. Other respondents mention that as opposed to previous GLs, here contractual standards apply to all TPAs (not just critical or important functions), which constitutes disproportionate burden for new and existing contracts. Some respondents raise that the provisions under points c, g, h are not always applicable and suggest clarifying that if a provision is not applicable, it can be omitted from the contract.	The Guidelines are consistent with the applicable DORA framework. The guidelines, as in the previous guidelines, distinguish between third party arrangement supporting critical or important functions and other arrangements.	No change No change
Contractual phase – DORA alignment (para. 85)	Several respondents stress that this paragraph should be more closely aligned with corresponding DORA provisions – ie. discrepancies in points b), e), f), h) and j) and also require avoiding the use of 'functions' provided by TPSPs (TPSPs provide services).	The comment has been accommodated and the Guidelines amended to be consistent with Article 30 (2) of DORA	The Guidelines have been amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Contractual phase – TPSP monitoring (para. 85j)	Several respondents ask for the removal of the requirement to monitor for all TPAs on ongoing basis (para. 85, point j)) as this would trigger significant increased workload in terms of updating contracts, and encourage greater proportionality as under DORA where the corresponding requirement is stated for critical functions only.	The comment has been accommodated and the Guidelines amended to be consistent with Article 30(2) and (3)(e) of DORA.	The Guidelines have been amended
Contractual phase – inspections (para. 86e)	Several respondents argue that the new provisions on access (unrestricted right of inspection and audit, obligation to cooperate, definition of scope and frequency of audits) result in disproportionate costs for FEs. They suggest either to limit these requirements to a monitoring right of the TPSP's performance on an ongoing basis or to apply it only to new contracts only on a risk-based approach.	This para. 86, point e) is only applicable to third party arrangements supporting critical or important functions and is consistent with DORA and international standards.	No change
Subcontracting of CIF – FE's responsibility (para. 88)	Several respondents request clarification regarding FE's responsibility and effective oversight beyond direct subcontractors	The use of subcontractors 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 supporting critical or important functions so that they are able to monitor, manage and mitigate those risks.	No change
Subcontracting of CIF – DORA alignment (Section 12.1)	Several respondents ask for the Guidelines to align the provisions on subcontracting to the wording used by DORA of subcontractors that "effectively underpin" services supporting critical or important functions, since not every	The Guidelines have been amended accordingly.	The Guidelines have been amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	subcontractor linked to a critical or important function plays a material role. They highlight that treating every subcontractor supporting a CIF as equal regardless of their importance or potential impact to the provision of the CIF diverges from a risk-based approach.		
Access and audit rights – contractual agreements (para. 97 and 100)	Some respondents ask clarification on whether access and audit rights must also be contractually agreed upon at non-critical levels.	For non-critical or non-important functions, it belongs to financial entities to consider whether including access and audit rights in the contractual arrangement (see para. 100 of the Guidelines) is necessary.	
	Several respondents suggest clarifying or deleting of 'becoming critical over time'. As an alternative, some respondents suggest specifying that audit rights should be included as a precautionary standard in all third-party arrangements, regardless of current criticality, while some others seek clarification that financial entities should be required to seek access only in cases where they reasonably believe the non-critical service may become critical over time.	The Guidelines follow the approach raised by respondents and para.100 should be understood in this way. See comment above.	No change
Access and audit rights – supervisory and resolution powers (para. 98)	Several respondents ask to restrict the provision to refer to supervisory and resolution powers to critical or important functions or to contracts that are relevant for resolution or resilience.	This paragraph is fully in line with the CRD and the BRRD frameworks.	No change
Monitoring – DORA alignment (para. 108)	A few respondents suggest alignment with DORA through the following changes: - removal of "where necessary"; - addition of "significant" before "breaches";	The comment has been accommodated.	The Guidelines have been amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	- addition of “evidenced” before “weaknesses.		
Monitoring – impediments to service (para. 109)	Several respondents stress that the wording under para. 109, point b) is too broad and ask for recognition of other mechanisms (SLA, etc) before termination. Some suggest addition of “materially negatively altering” or alignment with DORA, art. 28(7), point (c) “circumstances evidenced throughout monitoring deemed capable of altering performance”.	The comment has been accommodated and the Guidelines clarified to be consistent with Article 28 (7) of DORA.	The Guidelines have been amended
Monitoring – concentration risk (para. 114)	A few respondents suggest explicitly mentioning supply chains in this paragraph.	The comment has been accommodated.	The Guidelines have been amended
Exit strategies – CIF (para. 118)	Several respondents ask for limiting clearly exit strategies to critical or important functions at the beginning of para. 118, instead of point (b).	The Guidelines have been amended to align with the Article 28, para. 8 of DORA28 (8) DORA and only put in place exit strategies for services supporting critical or important functions.	The Guidelines have been amended
Exit strategies – business impact analysis (para. 119)	Several respondents flag that the provision to conduct a Business Impact Analysis on the exit strategy is an additional prescription with regards to DORA and ask for it to be removed.	See comment above. The comment has been accommodated and the requirement to perform a business impact analysis on the exit strategy deleted.	The Guidelines have been amended
Question 5. Is Annex I, provided as a list of non-exhaustive examples, appropriate and sufficiently clear?			
Mandatory non-exhaustive list	Several respondents expressed their concern regarding Annex I and its interpretation. They suggest clarifying that Annex I serves only as a tool providing illustrative examples of activities that could, in certain cases, be provided by TPSPs, and should not be interpreted as defining the scope of the Guidelines. The vast majority of respondents	Annex I has been deleted.	The Guidelines have been amended

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	consider the list of services in Annex I as too broad, extending the scope of the draft Guideline to services and functions which regularly do not have a material impact on financial entities'		
Critical or important Functions (CIFs)	For some respondents the list in Annex I, combined with the re-introduced 2019 criteria undermines DORA's principle-based approach, which intentionally simplified the identification of critical or important functions. Therefore, it should be clarified that Annex I should not serve as a parallel CIF test as reliance should rest solely on DORA's definition.	See above	The Guidelines have been amended